OA BOOKS

DATA FIDUCIARIES AND FAIR PLAY

Overcoming the Personal Data Protection Problem

GEORGE BOUCHAGIAR

The Canadian Center of Science and Education

Data Fiduciaries and Fair Play - Overcoming the Personal Data Protection Problem

By George Bouchagiar

DOI:10.5539/9780978430139

ISBN: 978-0-9784301-2-2 (print)

ISBN: 978-0-9784301-3-9 (ebook)

Published by Canadian Center of Science and Education

1120 Finch Avenue West

Suite 701-309

Toronto, ON., M3J 3H7

Canada

DATA FIDUCIARIES AND FAIR PLAY

Overcoming the Personal Data Protection Problem

GEORGE BOUCHAGIAR
INSTITUTE FOR INFORMATION LAW, AMSTERDAM, THE NETHERLANDS

Preface

Mass-consumed and mass-produced data are treated as an asset; a commodity that has fallen into the hands of intelligent machines and processors. Control over personal data is lost in an arena, where there is no room for secrecy. Technology meets mythology and equality is threatened as robots monitor, predict, and score people's behavior. While data's value is unequally distributed, people, not being parties to any agreement, get affected and influenced by powerful algorithms. The lack of control, the absence of secrecy, the unequal distribution of data's value, and the phenomenon of otherness, where non-parties may be affected, constitute four important aspects of the personal data protection problem. Some call for reconceptualization of privacy to end the game of poker, where individuals play with their hands open, whereas machines keep their cards close. Others demand fair compensation for personal data processing. In this study, a property rights-like approach is examined to determine whether and to what extent moral rights, sui generis rights, and trade secret rights could resolve the problem. As this approach would most probably fail to address all aspects of the problem, the introduction of trust via fiduciary laws is tested to overcome risks posed by Big Data and processing practices. Loyalty, trustworthiness, and care could be accompanied by duties of good faith and ethical conduct through a fair play-like approach that would bring fair information principles to the discussion table. Blockchains' potential is also examined; while these disruptive technologies are said to be extremely promising, this study finds that they would most probably be a bad fit for privacy. This makes fiduciary laws and fair play the key to reach the optimal result and overcome the above aspects of the personal data protection problem.

About the Authors

George Bouchagiar is an attorney-at-law, an author and a researcher.

He graduated from Athens Law School (Greece) and has earned a High Honors degree (Master of Science, Management of Cultural Property and New Technologies, Ionian University, Department of Archive, Library Sciences and Museology, School of Informatics and Information Science).

He has also completed a number of courses, including "Copyright for Educators & Librarians" and "Copyright for Multimedia" (Duke University, Emory University & The University of North Carolina at Chapel Hill), "Internet Giants: The Law and Economics of Media Platforms" (The University of Chicago), "America's Unwritten Constitution" and "America's Written Constitution" (Yale University), "Revolutionary Ideas: Utility, Justice, Equality, Freedom" (University of Pennsylvania), "Advertising and Society" (Duke University), "International Cyber Conflicts" (The State University of New York), "Philosophy and the Sciences: Introduction to the Philosophy of Cognitive Sciences" (The University of Edinburgh), "Children's Human Rights-An Interdisciplinary Introduction" (University of Geneva), "Constitutional Struggles in the Muslim World" (University of Copenhagen), "Introduction to Key Constitutional Concepts and Supreme Court Cases" (Penn University of Pennsylvania), "Corruption" (Wharton University of Pennsylvania), "Framework for data collection and analysis" (University of Maryland).

He has been practicing law since 2012 (privacy, data protection, intellectual property, internet law cases) and has been tutoring and lecturing as a research fellow (Information Law: Personal Data Protection/Intellectual Property; General Principles of Law) at the Ionian University (Department of Archive, Library Sciences and Museology, School of Informatics and Information Science) since 2018.

He has published a number of papers in national and international journals (on personal data, Big Data, intellectual property, commercial law, management of copyright, information law, competition law, fundamental human rights, art, public domain, etc) and has participated as a speaker at international conferences (on personal data, cloud computing, Intellectual Property). He has also organized (as chair of the organizing committee) national and international conferences (on bio-ethics, personal data, ICT) and has been a member of several associations (including International Society for Ethics and Information Technology, INSEIT – Hellenic Association of Data Protection and Privacy, HADPP – Information: History, Regulation, Culture, IHRC).

He is currently an internal trainee at IViR (Institute for Information Law, Amsterdam, The Netherlands).

More information available at https://www.georgeb.gr/.

This is for my mother and father.

Table of Contents

Chapter I. Introduction

Assume that one day back in 1995 someone told us that we no longer needed to pay for postal services; they would be offered for free. But the content of our letters would be accessible; the postal service providers would be able to read our messages[1].

Would we accept this?

In the age and the economy of Big[2] Data[3], information[4] is abundantly[5] available[6]. It is a mass-produced good that is consumed as a commodity rather than being used as a tool for personal growth or

[1] Seda Gürses & Bart Preneel, Cryptology and privacy in the context of big data, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, The Netherlands Scientific Council for Government Policy, WRR/Amsterdam University Press, The Hague/Amsterdam, 2016, pp. 49-86, at p. 56, mentioning that e-mails are postcards, not letters.

[2] The number of the traditional "3Vs" characteristics of Big Data (Volume, Variety and Velocity) is increasing; Variability, Veracity, Visualization, and –most importantly– Value have been added to the list. Tim Chartier, Vertigo Over the Seven V's of Big Data, The Journal of Corporate Accounting & Finance, Vol. 27, Issue 3, March/April 2016, pp. 81-82, at p. 81 (https://doi.org/10.1002/jcaf.22145), who also offers another "V" for Vertigo. Value is arguably the most interesting "V", as it includes societal value; Big Data may save human lives, improve maintenance, increase agricultural yields, or reduce traffic congestion. Peter Groves, Basel Kayyali, David Knott, Steve van Kuiken, The 'big data' revolution in healthcare: Accelerating value and innovation, January 2013, McKinsey & Company (available at https://www.ghdonline.org/uploads/Big_Data_Revolution_in_health_care_2013_McKinsey_Report.pdf); Jill Feblowitz, Analytics in Oil and Gas: The Big Deal About Big Data, March 2013, Society of Petroleum Engineers, SPE Digital Energy Conference, 5-7 March, The Woodlands, Texas, USA, doi: 10.2118/163717-MS (available at https://www.researchgate.net/publication/266662540_Analytics_in_Oil_and_Gas_The_Big_Deal_About_Big_Data); Alexandros Kaloxylos, Robert Eigenmann, Frederick Teye, Zoi Politopoulou, Sjaak Wolfert, Claudia Shrank, Markus Dillinger, Ioanna Lampropoulou, Eleni Antoniou, Liisa Pesonen, Huether Nicole, Floerchinger Thomas, Nancy Alonistioti, George Kormentzas, Farm management systems and the Future Internet era, Computers and Electronics in Agriculture, 2012, Vol. 89, pp. 130-144 (available at https://www.sciencedirect.com/science/article/pii/S0168169912002219); Saurabh Amin, Steve Andrews, Saneesh Apte, Jed Arnold, Jeff Ban, Marika Benko, Alexandre M. Bayen, Benson Chiou, Christian Claudel, Coralie Claudel, Tia Dodson, Osama Elhamshary, Chris Flens-Batina, Marco Gruteser, Juan-Carlos Herrera, Ryan Herring, Baik Hoh, Quinn Jacobson, Manju Kumar, Toch Iwuchukwu, James Lew, Xavier Litrico, Lori Luddington, JD Margulici, Ali Mortazavi, Xiaohong Pan, Tarek Rabbani, Tim Racine, Erica Sherlock-Thomas, Dave Sutter, Andrew Tinka, Ken Tracton, Olli-Pekka Tossavainen, Tom West, Arthur Wiedmer, Daniel B. Work, Qingfang Wu, Mobile Century, Using GPS Mobile Phones as Traffic Sensors: A Field Experiment, 15th World Congress on Intelligent Transportation Systems (November 16-20, 2008, New York), available at http://bayen.eecs.berkeley.edu/sites/default/files/conferences/its08.pdf. See also Samuel Fosso Wamba, Shahriar Akter, Andrew Edwards, Geoffrey Chopin, Denis Gnanzou, How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study, International Journal of Production Economics, Vol. 165, July 2015, pp. 234-246, at p. 235, who define Big Data as a "*holistic approach to manage, process and analyze 5 Vs (i.e., volume, variety, velocity, veracity and value) in order to create actionable insights for sustained value delivery, measuring performance and establishing competitive advantages*". Available at https://doi.org/10.1016/j.ijpe.2014.12.031.

[3] The term "data", which is derived from Latin, is the plural of "datum". This can be translated as "something given". Tobias M. Scholz, Big Data in Organizations and the Role of Human Resource

development of democratic societies[7]. Information, including personal[8] data[9], has acquired independent economic value[10] and, thus, new innovative business models[11] are emerging and dominating the market[12].

Management, A Complex Systems Theory-Based Conceptualization, 2017, Peter Lang GmbH, at pp. 9-12.

[4] Intangible information, like an idea when divulged, is non-excludable and non-rivalrous; its consumption by one person does not lessen another person's use and does not exclude others from using or getting access to this same information. Lawrence Lessig, Code, Version 2.0, Basic Books, 2006, pp. 180-185; J. Bradford DeLong & Lawrence Summers, The 'New Economy': Background, Historical Perspective, Questions and Speculations, Economic Review, Fourth Quarter 2001, Federal Reserve Bank of Kansas City, pp. 29-59 (available at https://www.kansascityfed.org/Publicat/econrev/Pdf/4q01delo.pdf). As Thomas Jefferson put it, "[…] *He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me* […]". Thomas Jefferson, letter to Isaac Mcpherson, August 13, 1813, Writings of Thomas Jefferson, 1790-1826, vol. 6, edited by H.A. Washington, 1854, at pp. 180-81.

[5] Greek term "πληροφορία" (i.e. "information") is derived from the terms "φέρω" (i.e. the verb "bear") and "πλήρης" (i.e. the adjective "full" or "complete"). The latter ("πλήρης") comes from the stem "plē-", which means "abundance". Iliana Araka, Nikos Koutras & Eliza Makridou, Access to information: Evolution and digital divide, in Maria Bottis (ed.), The history of Information: From papyrus to the electronic document, Nomiki Bibliothiki S.A., 2014, at pp. 398-399.

[6] As early as 2006, scholars spoke of "information overload". Kenneth Einar Himma, A Preliminary Step in Understanding the Nature of a Harmful Information-Related Condition: An Analysis of the Concept of Information Overload, Ethics and Information Technology, 2007, Vol. 9, No. 4, pp. 259-272.

[7] Kamiel J. Koelman, The Public Domain Commodified: Technological Measures and Productive Information Use, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain: Identifying the Commons in Information Law, 2006, Kluwer Law International, The Netherlands, pp. 105-119, at p. 105.

[8] "Personal data" means "[…] *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* […]". See Article 4(1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as "GDPR". In other jurisdictions, the term "personally identifiable information" is also used. Interestingly, in 2017, the European Commission proposed a Regulation as regards the free flow of non-personal data. See Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495), available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data.

[9] "[…] *Data is the fuel of the information economy, and the more data a company already has, the better it can monetize it* […]". Frank Pasquale, The Black Box Society, The Secret Algorithms that Control Money and Information, Harvard University Press, Cambridge, Massachusetts, London, England, 2015, at p. 141.

[10] Bernt Hugenholtz & Lucie Guibault, The Future of the Public Domain: An Introduction, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain, id, pp. 1-6.

[11] Barry Libert, Yoram (Jerry) Wind, and Megan Beck, What Airbnb, Uber, and Alibaba Have in Common, Nov. 20, 2014, Harvard Business Review, available at https://hbr.org/2014/11/what-airbnb-uber-and-alibaba-have-in-common, who distinguish four business models: asset builders (i.e. firms that

In a smart[13] new world[14] and in the advent of a post-information-revolution[15] era[16], when everything is measurable, people can be connected 24/7 through the Internet[17]. Big Data practitioners see themselves

---

build, develop, and lease physical assets, like FedEx); service providers (that hire employees who provide services or produce billable hours for which they charge, like JP Morgan); technology creators (meaning firms that develop and sell Intellectual Property, like software or biotechnology, e.g. Microsoft); and network orchestrators (who create a network of peers, where participants interact and share in the value creation, e.g. Alibaba).

[12] As some have put it, a business that owns no vehicles (e.g. Uber) may dominate the taxi market, while large hoteliers (e.g. Airbnb) may own no property. Simon Chesterman, Privacy and Our Digital Selves, The Straits Times, September 2, 2017 (available at https://ssrn.com/abstract=3033449), pp. 1-7, at p. 2. But Uber is not in the taxi market; it is in the business of selling consumers' data to a network of taxi-drivers and vice-versa, optimizing the taxi network by introducing greater data intelligence; and here the consumer is the product. Sander Klous, Sustainable Harvesting of the Big Data potential, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 27-46, at p. 27.

[13] Simply put, "smart" implies the addition of sensors, computational power, and network communications. Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, 2015, To Protect Personal Data, Support Innovation, Preserve Individual Liberties, at p. 35 ("From connected devices to autonomous devices: What freedoms subsist in a robotised world?").

[14] It is not only computers that are connected to the Internet, but also many objects communicate with each other in the environment of the Internet of Things. In this context, objects are connected to information networks. For instance, Radio-Frequency Identification enables wireless data collection by readers from electronic tags attached to or embedded in objects or even people. Pagnattaro Marisa-Anne, Getting Under Your Skin – Literally: RFID in the Employment Context, Journal of Law, Technology and Policy, No. 2, 2008, pp. 237-257, at p. 238 (available at https://ssrn.com/abstract=1565491). The so-called "smart grid" delivers electricity to consumers by using two-way digital technology to carry, not only electricity but also, information to and from peoples' houses. Quinn Elias Leake and Reed Adam, Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act (June 16, 2010), University of Colorado Law Review, Vol. 81, 2010, pp. 833-892 (available at https://ssrn.com/abstract=1625977). Such technologies may monitor individuals' activities in their home by collecting data, which may relate to vacation time or even caffeine consumption. Ann Cavoukian, Jules Polonetsky, Christopher Wolf, Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation, Identity in the Information Society, August 2010, Volume 3, Issue 2, Springer Link, pp. 275–294, available at https://link.springer.com/article/10.1007/s12394-010-0046-y. With regard to the increasing market of robots, which seem to appear in every home, see Calo Ryan, Robots and Privacy, in Patrick Lin, George Bekey, and Keith Abney (eds), Robot Ethics: The Ethical and Social Implications of Robotics, Cambridge, MIT Press, available at https://ssrn.com/abstract=1599189; Bill Gates, A Robot in Every Home, February 1, 2008, Scientific American, available at https://www.scientificamerican.com/article/a-robot-in-every-home-2008-02/.

[15] The information revolution has been defined as "[…] *a phenomenon whose consequences are unfolding in a space already shaped by thousands of other influences* […] *even though it was initiated by the recent technological development in information technologies, leading to the application of these technologies in 'all corners of society'* […]". Myriam Dunn Cavelty and Elgin M. Brunner, Introduction: Information, Power, and Security – An Outline of Debates and Implications, in Myriam Dunn Cavelty, Victor Mauer, Sai Felicia Krishna-Hensel (eds), Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, 2007, Ashgate, USA, England, pp. 1-18, at p. 4. Available at http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=F6EF124E3562F3A9354362CF1343A9B8?doi=10.1.1.466.3813&rep=rep1&type=pdf.

[16] Web 1.0 (First Era) corresponds to the early years of the World Wide Web. The web was a collection of mainly static pages that held information and content created by firms or organizations; the creation of content was performed by experts; users were mere information consumers. Web 2.0, the second generation of the Web, is defined by the empowerment of the end user to actively create content and

as data-scientists; the sexiest job of the 21st century[18]. Although the term 'big' in Big Data may be misleading, as no *big-messy*[19] data are needed when smart apps combine limited amounts of data for personalization[20], albeit, personal data are exchanged[21] and, thus, privacy[22] is threatened[23].

---

participate in the Web to expose herself and relate to others; attention is drawn to technologies that enable collaboration, such as social networks; tools are easy to use and this allows almost anyone to publish many different contents. Juan M. Silva, Abu Saleh Md. Mahfujur Rahman, Abdulmotaleb El Saddik, Web 3.0: A Vision for Bridging the Gap between Real and Virtual, in Proceedings of the 1st ACM international workshop on Communicability design and evaluation in cultural and ecological multimedia system, Vancouver, British Columbia, Canada, October 31, 2008, pp. 9-14, at p. 10; Federica Cena, Rosta Farzan Pasquale Lops, Web 3.0: Merging Semantic Web with Social Web, HT '09 Proceedings of the 20th ACM conference on Hypertext and hypermedia, Torino, Italy, June 29 - July 01, 2009, ACM, New York, pp. 385-386. Today, what we deal with is the Semantic Web (Web 3.0) that tries to extend models using a series of standard languages that enable the description of Web resources to be enriched and to become semantically accessible. Web 3.0 is based on two concepts: semantic tagging of resources, so that information can be understood by humans and computers, and the development of intelligent agents that are capable of operating with those resources and inferring new knowledge from them. To put it simply, the Semantic Web adds meaning to web documents from the sense of content and metadata. See, amongst others, Tim Berners-Lee, James Hendler, Ora Lassila, The Semantic Web, Scientific American, Vol. 284, No. 5 (May 2001), pp. 34-43; J. Hendler, Agents and the semantic web, IEEE Intelligent Systems, Volume 16, Issue 2, Mar-Apr 2001, pp. 30–37; J. M. Morales-del-Castillo, Eduardo Peis, Antonio A. Ruiz, E. Herrera-Viedma, Recommending biomedical resources: A fuzzy linguistic approach based on semantic web, International Journal of Intelligent Systems, Vol. 25, Issue 12, Special Issue: New Trends for Ontology-Based Knowledge Discovery, December 2010, pp. 1143-1157; Bujar Raufi, Florije Ismaili, Jaumin Ajdari, Xhemal Zenuni, Knowledgebase Harvesting for User-Adaptive Systems Through Focused Crawling and Semantic Web, in Proceedings of the 17th International Conference on Computer Systems and Technologies 2016, Palermo, Italy (June 23-24, 2016), pp. 323-330, at p. 324 (where it is also mentioned that "[…] *semantic web tends to add semantic meaning or metadata to every document on the web so they can be machine processable as well as easily retrievable. The Semantic Web brings structure to the meaningful content of Web pages, creating an environment where different software agents such as crawlers can move around from page to page and can readily carry out sophisticated tasks for users. The process of publishing a meaningful content to the web requires a confluence between users as well as adjusting to frequent technology changes related to semantic web* […]"). In this context, individuals are no longer users; they are part of the applications that emerge and disappear; they are also producers, subjects and beneficiaries of the Big Data. David Kreps, Kai Kimppa, Theorising Web 3.0: ICTs in a changing society, Information Technology & People, 2015, Vol. 28, Issue 4, pp. 726-741, at p. 734.

[17] See, in general, Viktor Mayer-Schonberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, And Think, Eamon Dolan/Mariner Books, 2014 (reprint edition).

[18] Thomas H. Davenport & D.J. Patil, Data Scientist: The Sexiest Job of the 21st Century, Harvard Business Review, October 2012 Issue. Available at https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century.

[19] Mike Wheatley, Big, Messy Data & The Internet Of Things, September 19, 2013, SiliconAngle, available at https://siliconangle.com/blog/2013/09/19/big-messy-data-the-internet-of-things/; Sam Ransbotham, The Smart Way to Deal With Messy Data, December 20, 2016, MIT Sloan Management Review, available at https://sloanreview.mit.edu/article/the-smart-way-to-deal-with-messy-data/.

[20] Take, for example, the quantified self that incorporates technology into data acquisition on aspects of a person's daily life. Gary Wolf, The Data-Driven Life, April 28, 2010, The New York Times, available at https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html.

[21] In 1992, it was estimated that data traders exchanged personal data every five seconds. Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, The Yale Journal of International Law, 2000, Vol. 25, pp. 1-88, at p. 2 (available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1112&context=yjil).

As firms[24] process raw[25], unstructured[26], but also personal[27] data[28] derived from innumerous sources[29], users' control over their information is lost. Sensitive information may be exchanged[30] or further

---

[22] See Article 8 of the European Convention on Human Rights; Judgment of the European Court of Human Rights (Fourth Section), Case of *Peck v. The United Kingdom* (Application no. 44647/98), 28 January 2003, paragraph 57 ("[…] *Private life is a broad term not susceptible to exhaustive definition* […] *The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'* […]"). In this context, the 'individual sector' is protected; the 'zone of individual power' necessary for the healthy development and functioning of the individual and absolutely essential to the health and survival of democratic societies. Charles A. Reich, The Individual Sector, The Yale Law Journal, 1991, Vol. 100, pp. 1409-1448, at pp. 1409, 1410, 1442.

[23] To some, privacy is understood as the protection of the integrity of the individual self as composed of multitude of identities (e.g. the individual as a consumer). So, data use may become intrusive when it discloses the subject's personality as expressed through her consumer self. As Karas puts it, an accurate record of our purchases can produce a blurry but strikingly accurate glance at our private selves. Stan Karas, Privacy, Identity, Databases, in American University Law Review, 2002, Vol. 52, No. 2, pp. 393-445, at pp. 398, 429.

[24] Firms treat data as their property or even as their "speech". Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 2000, Stanford Law Review, Vol. 52, pp. 1373-1437, at p. 1375.

[25] In the age of the semantic web importance is attached to raw data, which are collected from different sources to discover, assemble and correlate a huge volume of information. Maria Giannakaki, The value of information in the age of 'Big Data': from Web 1.0 to Web 3.0, in Maria Bottis (ed.), The history of Information: From papyrus to the electronic document, id, pp. 259-272.

[26] In 2010, only 5 percent of all digital data was "structured"; the remaining 95 percent was unstructured data, such as web pages or video. Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, id, at p. 47.

[27] See, for example, Randal C. Picker, Competition and Privacy in Web 2.0 and the Cloud, Northwestern University Law Review Colloquy, 2008, Vol. 3, No. 1 (available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1147&context=journal_articles); Omer Tene, What Google knows: Privacy and Internet search engines, Utah Law Review, 2008, Vol. 4, pp. 1434-1492.

[28] In fact, ordinary life contains innumerous online activities during which an unprecedented volume of data is produced and processed (Committee on Commerce, Science, and Transportation, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, Dec. 18, 2013, available at http://educationnewyork.com/files/rockefeller_databroker.pdf). One could question whether someone's, e.g., "heart rate", when recorded by a smart app, is personal data. But in the age of Big Data the collection and processing of a huge volume of data allows identification of a natural person. Provided that a datum relates to a natural person, who can be identified, it is personal. And any natural person can be identified by several means. Judgement of the Court of Justice of the European Union (6 November 2003), Case C-101/01, Criminal proceedings against *Bodil Lindqvist*, EU:C:2003:596, paragraph 27. In this context, even IP addresses and cookies are treated as personal data (Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, June 20, 2007; Opinion 1/2008 on data protection issues related to search engines, April 4, 2008; Patrick Lundevall-Unger and Tommy Tranvik, IP Addresses – Just a Number?, International Journal of Law and Information Technology, 2010, Vol. 19 No. 1, Oxford University Press, doi:10.1093/ijlit/eaq013, pp. 53-73). Simply put, the criterion that has to be met and that makes the data personal is the capacity to identify a person (Omer Tene, What Google knows: Privacy and Internet search engines, id, at p. 1446).

[29] Omer Tene, Privacy: The New Generations, International Data Privacy Law, Vol. 1, Issue 1, 1 February 2011, pp. 15–27. Available at https://academic.oup.com/idpl/article/1/1/15/759641.

processed[31] and some scholars speak of theft of personal property[32]; others argue that we should receive fair compensation for the use of our data[33]. As secrecy is absent, transactions between users and Big Data platforms have been regarded as a game of poker, where the individual has her hand open and the platform keeps its cards close[34]. In an environment where technology and "mythology" may blend together[35], machines or robots[36] may monitor and predict phenomena and patterns[37]. And this can lead to societal benefits[38]. But they also predict and monitor people's behavior[39] and this may increase

---

[30] Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain, id, pp. 223-257, at p. 228; Chris Jay Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, N.C. J. Int'l L. & Com. Reg., 2003-2004, Vol. 29, pp. 595-637, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1677&context=facpubs; Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, California Law Review, 2008, Vol. 96, Issue 4, pp. 901-966, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1169&context=californialawreview.

[31] Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, Boston College Law Review, Vol. 55, Issue 1, 2014, pp. 93-128.

[32] Steve Mann, Computer Architectures for Protection of Personal Informatic Property: Putting Pirates, Pigs, and Rapists in Perspective, First Monday, Vol. 5, No. 7, July 2000 (available at http://firstmonday.org/ojs/index.php/fm/article/view/774/683).

[33] Jessica Litman, Information Privacy/Information Property, Stanford Law Review, 2000, Vol. 52, pp. 1283-1313. As Laudon put it, "[…] *There should be no free lunch when it comes to invading privacy* […]". Kenneth C. Laudon, Markets and Privacy, Vol. 39, Issue 9, Communications of the ACM, 1996, pp. 92-104, at p. 103 (available at https://dl.acm.org/citation.cfm?id=234476).

[34] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, 2013, Vol. 11, Issue 5, pp. 239-273, at p. 255. As some have questioned, since credibility of those who advocate monitoring increases to the extent that they are willing to apply same technologies to themselves, why not let firms collect personal data on condition that their top 100 officers must post exactly the same data about themselves and their family members on an accessible website? For a discussion on this view, see David Brin, The Transparent Society: Will technology Force Us to Choose Between Privacy and Freedom?, Basic Books, 1998, US, at p. 81.

[35] danah boyd & Kate Crawford, Critical Questions For Big Data, Information, Communication & Society, 2012, Vol. 15, No. 5, pp. 662-679, available at https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2012.678878, at p. 663, defining Big Data as a cultural, technological, and scholarly phenomenon that rests on the interplay of technology (maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets), analysis (drawing on large data sets to identify patterns to make economic, social, technical, and legal claims), and mythology (i.e. the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy).

[36] Robots are becoming *cobots* (collaborative robots) that can act with humans. To do so, they collect far more data. This highlights a fundamental ethical paradox in the data protection domain: to be more autonomous, a machine must become more dependent on personal data. Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, id, at p. 36.

[37] Gregory D. Abowd & James P. G. Sterbenz, Final report on the inter-agency workshop on research issues for smart environments, IEEE Personal Communications, October 2000, Vol. 7, Issue 5, pp. 36-40. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=878535.

[38] Namely, it may be a matter of time before cancer is transformed from a killer into a chronic disease. Chetan Bettegowda et al., Detection of circulating tumor DNA in early- and late-stage human malignancies, Science Transnational Medicine, 2014, Vol. 6, Issue 224, available at https://www.researchgate.net/publication/260271031_Detection_of_Circulating_Tumor_DNA_in_Early-_and_Late-Stage_Human_Malignancies.

inequality and threaten democracy[40]. And while the unequal distribution of data's value is acknowledged, people, not being parties to any contract or agreement, can be affected by powerful algorithms[41] and their automated decision-making.

So, the absence of control, the lack of secrecy, the unequal distribution of data's value, and the phenomenon of otherness, where non-parties may be affected, are four important aspects of the personal data protection problem.

In Part II, personal data processing is examined to better understand the extent to which privacy can be threatened.

Further analysis of the above four aspects is conducted in Part III to specify the personal data protection problem.

In Part IV, the potential introduction of property rights in data is examined. As such items of information are intangible attention is drawn to Intellectual Property rights. A moral rights-like approach may strengthen the individuals' control and could perhaps address the aspect of the lack of secrecy. These rights, being enforceable against any person beyond those with whom an individual may contract, could also resolve the problem of otherness. But moral rights refer to products of the human mind and are not supposed to function as commodities. As data may be regarded as the asset or the content of a private database, *sui generis* rights are also tested to argue that people's data have, in many cases, fallen into the wrong hands. Before leaving the sphere of property, trade secrecy is examined. While a *quasi* trade secret right in personal data could strengthen the individuals' control or keep information secret, albeit it would most probably fail to address the aspect of otherness; it would not be asserted against those who process data but are often not in privity with the data subject.

As a property-like approach might also raise policy or free speech issues, fiduciary laws are proposed in Part V to establish trust. Data processors could be regarded as fiduciaries, as they have special power over (and special relationship to) others. Maybe, the duty of loyalty and trustworthiness would ensure that the processor would act in the interest of the beneficiary. A duty of care, a duty to act diligently, might also strengthen the position of individuals, who are ill-prepared to monitor the data processors' behavior. Vulnerability, dependence, and the experts' awareness of possessing valuable data could justify the implementation of fiduciary laws.

---

[39] Software and hardware determine our behavior probably more than laws. See, in general, Evgeny Morozov, The Net Delusion, The Dark Side of Internet Freedom, 2011, Public Affairs, USA. To some, code is law. Lawrence Lessig, Code, Version 2.0, id. And this is no bad thing, as we may change the code. But when a system becomes the equivalent of the law, the system developer becomes the legislator. Mireille Hildebrandt, Criminal Law and Technology in a Data-Driven Society, 2014, The Oxford Handbook of Criminal Law, Oxford University Press, pp. 174-197.

[40] Cathy O'Neil, Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy, 2016/2017, Broadway Books, NY.

[41] Simply put, an algorithm is defined by a sequence of steps and instructions that can be applied to data. Algorithms generate categories for filtering information, operate on data, look for patterns and relationships, or, generally, assist in analysis of information. John Podesta, Penny Pritzker, Ernest J. Moniz, John Holdren, Jeffrey Zients, Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, May 2014, The White House, Washington, at p. 46. Available at https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

In Part VI, duties of good faith and ethical conduct, which are owed to the members of society as a whole, are examined via a fair play-like approach.

In Part VII, latest technologies' potential is tested to draw final conclusions. While many authors argue for the promises of blockchain in several fields, its real and emergent properties are distinguished from one another to conclude that "chains" would most probably be a "bad fit" for addressing the personal data protection problem.

Chapter II. Personal Data Processing: A Direct Violation of Privacy?

Information has many facets[42] and has been viewed as (to name but a few) a weapon[43], a critical resource[44], a realm (like space)[45], an environment (the "infosphere")[46], a medium for military operations (like air power)[47], a catalyst[48], or a control parameter in a process[49]. To some[50], information

[42] Capurro and Hjørland argue that one should see the concept of information, not in isolation but, in relation to other concepts, like documents and media. Rafael Capurro & Birger Hjørland, The Concept of Information, in Annual Review of Information Science and Technology, B. Cronin (ed.), Vol. 37 (2003), Chapter 8, pp. 343-411, at p. 396, available at http://www.capurro.de/infoconcept.html#How.

[43] Laura Saunders, Information as Weapon: Propaganda, Politics, and the Role of the Library, in ACRL 2013, April 10-13, Indianapolis, IN, pp. 309-318. Available at http://www.ala.org/acrl/sites/ala.org.acrl/files/content/conferences/confsandpreconfs/2013/papers/Saunders_Information.pdf.

[44] William R. King, Varun Grover, Ellen H. Hufnagel, Using information and information technology for sustainable competitive advantage: Some empirical evidence, in Information & Management, Vol. 17, Issue 2, September 1989, pp. 87-93, at p. 88 (available at https://www.sciencedirect.com/science/article/pii/0378720689900104); J. Yannis Bakopoulos, Toward a More Precise Concept of Information Technology, Association for Information Systems (AIS Electronic Library, AISeL), ICIS 1985 Proceedings, International Conference on Information Systems (ICIS), pp. 17-24, at pp. 19-20, who defines information technology as the "[…] *set of non-human resources dedicated to the storage, processing and communication of information, and the way in which these resources are organized into a system capable of performing a set of tasks* […]" (available at https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1022&context=icis1985).

[45] David Brin, The Transparent Society, id, at p. 316, citing Jeffrey Cooper.

[46] Luciano Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, 2014, Oxford University Press, pp. 1-272.

[47] Richard M. Jensen, Information War Power: Lessons from Air Power, Program on Information Resources Policy, Harvard University, Center for Information Policy Research, 1997, at p. 13 (speaking of "information manipulation", which involves the four "D's": degradation, disruption, denial, and destruction of enemy information). Available at http://www.pirp.harvard.edu/pubs_pdf/jensen/jensen-p97-2.pdf.

[48] Adina-Petruta Pavel, Andreas Fruth, Monica-Nicoleta Neacsu, ICT and E-Learning – Catalysts for Innovation and Quality in Higher Education, 2nd Global Conference on Business, Economics, Management and Tourism, 30-31 October 2014, Prague, Czech Republic, Procedia Economics and Finance, Volume 23 (2015), pp. 704-711, available at https://ac.els-cdn.com/S2212567115004098/1-s2.0-S2212567115004098-main.pdf?_tid=0e3262be-9ee5-4476-b622-a4eed62af436&acdnat=1529104704_3ac9c60b934d42c85c692c8f130b0980; Fermin G. Castillo, Information and Communication Technology In Today's Modern Education, Second International Conference on Engineering System Management and Applications, 30 March-1 April 2010, Sharjah, United Arab Emirates, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5700041.

[49] James Gleick, The Information, A History, A Theory, A Flood, 2011, Pantheon Books, New York. To Gleick, information is what our world runs on, "*the blood and the fuel, the vital principal*" (James Gleick, id, at p. 8).

[50] Luciano Floridi, Information ethics: On the philosophical foundation of computer ethics, Ethics and Information Technology, Vol. 1 (1999), Kluwer Academic Publishers (The Netherlands), pp. 37-56, at p. 43. Available at http://blogs.oii.ox.ac.uk/floridi/wp-content/uploads/sites/67/2014/05/ieotfce.pdf.

is not just about "life" (persons, animals, plants and so forth), but also about anything that exists (e.g. paintings, stars, or stones), anything that may exist (e.g. future generations), and anything that exists no more (such as our ancestors). The digital environment, because of the intangible nature of information and the virtual interaction with faceless individuals, may be regarded as a magical, dream-like, environment that has nothing to do with the real world[51].

Today, the distinction between offline and online life has become completely blurred: they have become one[52]. And maybe what we do not see is that instead of the digital world becoming more like the real world, the real world is becoming more like the digital. It may seem awkward to talk about the Internet[53] as a "new technology" these days[54], but it has undeniably changed the rules. Our lives are uploaded on devices[55] and things[56], things that used to be blind and mute but which now talk, hear or think[57]; and information is exchanged without the individuals' control[58]. For instance, an alarm clock

[51] Luciano Floridi, Information ethics: On the philosophical foundation of computer ethics, id, at p. 40, mentioning that a person may wrongly infer that "[…] *her actions are as unreal and insignificant as the killing of enemies in a virtual game* […]".

[52] Lambèr Royakkers, Jelte Timmer, Linda Kool, Rinie van Est, Societal and ethical issues of digitization, in Ethics and Information Technology, June 2018, Volume 20, Issue 2, pp. 127-142, at p. 128. As the authors put it, digitization has allowed technology to nestle itself both in us (e.g. via implants) and between us (e.g. via social networks) and to know more about us (e.g. via Big Data) or learn to behave like us (e.g. via robots). See Lambèr Royakkers, Jelte Timmer, Linda Kool, Rinie van Est, id, at p. 127.

[53] To some, the Internet is the most important human advancement since the printing press or even the most important discovery since fire. See, amongst others, John Barlow, A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, Feb. 9, 1996. To others, the Internet is a cynical cosmos, designed along cynical principles to serve cynical ends better than any others. See Siva Vaidhyanathan, The Anarchist in the Library: How the Clash Between Freedom and Control Is Hacking the Real World and Crashing the System, Basic Books, 2004, at pp. 26-27, where the author brilliantly argues that Diogenes of Sinope was a hacker, expressing his freedom by masturbating in the marketplace; and nothing represents the overall nature of the Internet better than "*masturbating in the marketplace*".

[54] Omer Tene, Privacy: The New Generations, in International Data Privacy Law, 2011, Vol. 1, No. 1, pp. 15-27, at p. 16.

[55] For some statistics as regards data processing and collection, smart environments, mobile tracking, and relevant privacy-related technologies, see Charles Raab & Ivan Szekely, Data protection authorities and information technology, Computer Law & Security Review, 2017, Vol. 33, Issue 4, pp. 421-433, at pp. 428, 429.

[56] The "Internet of Things" (IoT) can be defined as a network of physical objects (e.g. devices, vehicles or even buildings) embedded with sensors, software or network connectivity that enable those objects to collect, store and exchange data. See Otto Petrovic, The Internet of Things as Disruptive Innovation for the Advertising Ecosystem, in Gabriele Siegert, M. Bjørn von Rimscha, Stephanie Grubenmann (eds), Commercial Communication in the Digital Age, Information or Disinformation?, de Gruyter GmbH, 2017, pp. 183-205, at p. 187. For instance, a modern intelligent connected car can be defined as a computer system similar to a smart phone, controlled by a complex computer with a wireless communication network and internal in-vehicle network. Kim Shiho, Blockchain for a Trust Network Among Intelligent Vehicles, Advances in Computers, 2018, pp. 2-26 at p. 2 (available at https://www.sciencedirect.com/science/article/pii/S0065245818300238 - https://doi.org/10.1016/bs.adcom.2018.03.010).

[57] Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman, FairAccess: A new Blockchain-based access control framework for the Internet of Things, Security and Communication Networks, December 2016, Vol. 9, No. 18, pp. 5943-5964, at p. 5943. See also at pp. 5945-5947, where (as regards the Internet of Things) transparency is defined as helping people understand who knows what about them, how data are used, with whom they are shared, and how long they are held; pseudonymity is regarded as a trade-off anonymity with accountability, where actions of a person are linked with a

may perform its additional roles as a coffee machine or a heart-beat measurer and constantly accompany a person, while a smart fridge can "paternalistically"[59] change the order of one's favorite milk, due to her high cholesterol levels.

One could fairly claim that we are moving towards a direction, where people make use of services instead of buying products; we no longer buy a map or a washing machine, but we use map-apps or washing services. This has led to a "servitization" or a "digital feudalism"[60], where people's ownership over themselves has been lost[61].

And it has been officially recognized that consumers pay for such services with their data[62]. In fact, personal data are processed on a daily basis, as one exchanges e-mails and messages[63], uses her mobile device[64], uploads files on the Cloud[65], or measures herself during everyday activities[66].

---

pseudonym, a random identifier, rather than an identity; confidentiality is understood as no unauthorized disclosure of resources; integrity is treated as no improper modification of resources; and reliability is a situation to which the continuity of a service leads. The authors classify IoT devices in "personal/home", "government/utilities", and "enterprise/industry".

[58] See Debjanee Barua, Judy Kay & Cecile Paris, Viewing and Controlling Personal Sensor Data: What do Users Want?, in Persuasive'13, Proceedings of the 8th international conference on Persuasive Technology (Sydney, NSW, Australia - April 03-05, 2013), pp. 15-26, at pp. 24-25, mentioning that even basic levels of control may not be supported by current sensors, as every sensor and its associated data are under the control of its manufacturer. See also Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review, 2014, Vol. 93, pp. 85-176, at p. 160; Eric Barbry, The Internet of Things, Legal Aspects: What Will Change (Everything)…, in Communications & Strategies, Digiworld Economic Journal, no. 87, 3rd Q. 2012, pp. 83-100, at p. 84, arguing that the Internet of Things aims to make things intelligent and serve as a true decision-making tool "[…] *going as far as replacing human decision* […]". Roman, Zhou and Lopez argue that information providers not only have their own access control policies and permissions but also control the granularity of the data they produce. See Rodrigo Roman, Jianying Zhou, Javier Lopez, On the features and challenges of security and privacy in distributed internet of things, in Computer Networks, 2013, Volume 57, Issue 10, pp. 2266-2279, at pp. 2273, 2275. Available at https://www.sciencedirect.com/science/article/pii/S1389128613000054.

[59] Lorenz Hilty, Ethical issues in ubiquitous computing - three technology assessment studies revisited, in Kinder-Kurlanda, Katharina & Ehrwein Nihan, Céline, Ubiquitous Computing in the Workplace, 2015, Cham: Springer, pp. 45-60, at pp. 52-53. Hilty argues that paternalism may be "*delegated*" to machines by technology and, when executed by machines, is called technology paternalism.

[60] Sascha D. Meinratht, James W. Losey & Victor W. Pickard, Digital Feudalism: Enclosures And Erasures From Digital Rights Management To The Digital Divide, Commlaw Conspectus, 2011, Volume 19, pp. 423-479. Available at https://scholarship.law.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1470&context=commlaw.

[61] John Podesta, Penny Pritzker, Ernest J. Moniz, John Holdren, Jeffrey Zients, Big Data: Seizing Opportunities, Preserving Values, id, at p. 9, mentioning that "[…] *more and more data will be generated about individuals and will persist under the control of others* […]". See also Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, Journal of Information Technology, 2015, Volume 30, pp. 75-89 (available at https://ssrn.com/abstract=2594754).

[62] See European Commission's press release on the 27th of June 2017 ("[…] *Google's flagship product is the Google search engine, which provides search results to consumers, who pay for the service with their data* […]"), available at http://europa.eu/rapid/press-release_IP-17-1784_en.htm; Article 3(1) of the Proposal of the European Commission for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content [(COM(2015)0634 – C8-0394/2015 – 2015/0287(COD)], where it is mentioned that "[…] *This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in*

But does this really matter? Since it is a firm's "machines" (rather than its employees) the ones seeing a person's information, why does she need to worry? Is this not as she was standing naked in front a cat? No, it is not. The cat does not remember (the way machines remember); the cat does not understand (the way machines understand); it does not process, nor does it base its decisions on what it sees (to the extent machines do). The cat will not tell anyone, albeit machines communicate[67].

"*But, if you do nothing wrong, you have nothing to hide*". This is not true; when we make love, we do nothing wrong[68]. Besides, if one has nothing to hide then he does not have a life[69].

So, how far has data collection gone?

Supermarkets collect data from consumers to offer personalized coupons[70]; they have been undertaking similar actions since (at least) 1998[71]. Some firms, monetizing a commodity people produce just by

---

exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data […]"; Report of the European Parliament on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (where the proposal's title is amended to include "contracts for the supply" of digital services), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2017-0375%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN. See also Bureau Européen Des Unions De Consommateurs (BEUC), Digital Content Directive, Key recommendations for the trialogue negotiations (22/01/2018), available at http://www.beuc.eu/publications/beuc-x-2018-003_digital_content_directive.pdf.

[63] Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at p. 229.

[64] See, for instance, Google's terms of use: https://www.google.com/policies/privacy/.

[65] Herrick Lidstone, Using the Cloud: Trade Secrets and Confidential Information Aren't So Secret, Burns, Figa & Will, P.C. 2014 (available at https://ssrn.com/abstract=2358472; http://dx.doi.org/10.2139/ssrn.2358472); Evgeny Morozov, The Net Delusion, id, at p. 286.

[66] Tara Brabazon, Digital Fitness: Self-Monitored Fitness and The Commodification Of Movement, Communication Politics & Culture, Vol. 48, No. 2, 2015, Flinders University, available at https://pdfs.semanticscholar.org/b787/d0441558f14a8c6af046625adf1e9afd725a.pdf; Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, id, at p. 94 (speaking of a disparate group of fitness aficionados and some tech junkies, who measure their bodies and lives to live better).

[67] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, 2015, W.W. Norton & Company, New York, at p. 153. For instance, intelligent connected vehicles communicate with almost all systems and devices in cyberspace, even those existing offline (e.g. offices and houses). See Kim Shiho, Blockchain for a Trust Network Among Intelligent Vehicles, id, at p. 5.

[68] Bruce Schneier, Data and Goliath, id, at p. 147.

[69] Daniel J. Solove, Nothing to Hide: The False Tradeoff between Privacy and Security, 2011, Yale University Press, at p. 21.

[70] Katherine Albrecht, Supermarket Cards: The Tip of the Retail Surveillance Iceberg, Denver University Law Review, 2002, Vol. 79, Issue 4, pp. 534-539.

[71] David Brin, The Transparent Society, id, at p. 8 (mentioning that cash register scanners in supermarkets, video stores and pharmacies collect consumers' data to serve them "more efficiently").

living their lives, collect data to create private networks of knowledge[72]. Others not only collect but also produce personal data, after having found ways to determine that a consumer is pregnant[73]. Data mining[74] companies, owning some two and a half million Gigabytes databases of consumers' information[75], may help other firms target individuals and promote their marketing strategies via

[72] Julia Powles & Hal Hodson, Google DeepMind and healthcare in an age of algorithms, Health and Technology, 2017, Vol. 7, Issue 4, pp. 351-367, available at https://link.springer.com/article/10.1007/s12553-017-0179-1.

[73] Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, id, at pp. 94, 95, 98. Interestingly, Target's statisticians claim that they can assign each consumer "a pregnancy prediction score" and also estimate her due date to send coupons timed to very specific stages of her pregnancy. See Charles Duhigg, How Companies Learn Your Secrets, The New York Times Magazine, Feb. 16, 2012, available at https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Examples of sensitive data processing are not few: Jeffrey A. Dretler, United States: Collection Of Biometric Data Raises Privacy Concerns For Employees And Compliance Issues For Employers, March 16, 2018, Mondaq, available at http://www.mondaq.com/article.asp?articleid=683572&email_access=on&chk=2220404&q=1536832; Matt Rosoff, Facebook is facing its biggest test ever—and its lack of leadership could sink the company, March 18, 2018, CNBC, available at https://www.cnbc.com/2018/03/18/facebook-failing-zuckerberg-and-sandberg-absent-commentary.html?utm_source=pocket&utm_medium=email&utm_campaign=pockethits; Daphne Keller, Data Analytics, App Developers, and Facebook's Role in Data Misuse, March 20, 2018, Stanford Law School, available at https://law.stanford.edu/2018/03/20/data-analytic-companies-app-developers-facebooks-role-data-misuse/; Thibaut D'hulst, Van Bael & Bellis, Belgium: Brussels Court Finds Facebook Cookies In Breach Of Data Protection Laws And Imposes € 250,000 Daily Penalty To End Infringement, Mondaq, March 27, 2018, available at http://www.mondaq.com/article.asp?articleid=686834&email_access=on&chk=2223666&q=1536832; Jennifer Kulynych & Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research when Privacy and Science Collide, 3 Journal of Law and the Biosciences, January 15, 2017, pp. 94-132, at p. 119 (mentioning that "[…] *the federal HIPAA Privacy Rule permits entities covered by the Privacy Rule (most health care providers, insurers, and pharmacies) to use or share identifiable patient information without consent to provide treatment. Covered entities may also use identifiable patient information internally, without consent, as necessary to conduct normal business operations* […] *the Privacy Rule also permits 'covered entities' to disclose or share patient information, also without consent, with other covered entities for treatment or reimbursement purposes, and with vendors and contractors who sign an agreement* […]"), available at https://law.stanford.edu/publications/clinical-genomics-big-data-and-electronic-medical-records-reconciling-patient-rights-with-research-when-privacy-and-science-collide/.

[74] Data mining can be defined as the exploration and analysis of large quantities of data to discover meaningful patterns and rules. Michael J.A. Berry, Gordon S. Linoff, Data Mining Techniques for Marketing Sales, and Customer Relationship Management, Second Edition, Wiley, 2004, pp. 1-643, at p. 7 (mentioning that although data mining may improve a firm's market, services, and customer support operations through a better understanding of its clients, albeit hardly any of the data mining algorithms were first invented with commercial applications in mind). Fulda has defined "data mining" as the intelligent search for new knowledge in existing masses of data. Joseph Fulda, Data Mining and Privacy, in Albany Law Journal of Science & Technology, 2000, Vol. 11, pp. 105-113, at p. 106. The primary benefit of data mining is a firm's ability to increase profits. Morgan Hochheiser, The truth behind data collection and analysis, The John Marshall Journal of Information Technology & Privacy Law, 2016, Vol. 32, pp. 32-54, at p. 39 (see also at pp. 51-52, where opt-in programs and fixed fines and penalties are proposed to protect consumers).

[75] Doug Henschen, Catalina Marketing Aims For The Cutting Edge Of 'Big Data', Jun. 9, 2011, InformationWeek, available at https://www.informationweek.com/big-data/big-data-analytics/catalina-marketing-aims-for-the-cutting-edge-of-big-data/d/d-id/1099971. See also Catalina Marketing's website at https://www.catalina.com/insights/.

personal data analysis[76]. Credit-card transaction records may be used to prove that online ads are prompting people to make purchases even when they happen in brick-and-mortar stores[77].

As some have aptly put it, what we deal with today is the monster of a free Internet[78] paid for by advertising targeted on the basis of an unprecedented level of surveillance[79] of human lives[80]. Data processing enables firms and organizations to identify an individual, detect her activities[81], profile

[76] Eric Siegel, Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, Revised and Updated, 2016, Wiley, pp. 1-368, at p. 25, observing that each application of predictive analytics is defined by: what is predicted, meaning the kind of behavior, i.e. action event, or happening, to predict for each person, stock or other kind of element; and what is done about it, meaning the decisions driven by prediction, the action taken by the organization in response to or informed by each prediction.

[77] Elizabeth Dwoskin, Craig Timberg, Google now knows when its users go to the store and buy stuff, May 23, 2017, The Washington Post, available at https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?utm_term=.b97032baeb8b. Google's program (Store Sales Measurement) matches goods, which are purchased in traditional stores, to the "clicking" of online ads ("Bricks to Clicks"). Thus, the firm is aware of whether a consumer bought the product, on the ad of which she clicked. In 2017, the Electronic Privacy Information Center (EPIC) asked the Federal Trade Commission (FTC) to examine lawfulness of Google's program. Brian H. Lam and Cynthia J. Larose, United States: FTC Asked to Investigate Google's Matching Of Bricks To Clicks, September 25, 2017, Mondaq, available at http://www.mondaq.com/article.asp?articleid=630914&email_access=on&chk=2167746&q=1536832. Recently, Google reported that, in 2017, it took down more than 3.2 billion ads that violated its advertising policies. This included 79 million ads, which aimed to send people to malware-laden sites, 66 million "trick-to-click" ads, and 48 million ads, which attempted to get people to install unwanted software. Google also reported that it blocked 320,000 publishers and blacklisted about 90,000 websites and 700,000 mobile apps for violating Google's policies. Scott Spencer, An advertising ecosystem that works for everyone, Google, Mar. 14, 2018, available at https://blog.google/topics/ads/advertising-ecosystem-works-everyone/.

[78] Neil M. Richards & Jonathan H. King, Big Data and The Future for Privacy, Handbook of Research on Digital Transformations, Elgar, 2016, pp. 1-26, at p. 11. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2512069.

[79] Glen Whelan, Trust in Surveillance: A reply to Etzioni, Journal of Business Ethics, 2018, Springer, The Netherlands, pp. 1-5, available at https://link.springer.com/article/10.1007/s10551-018-3779-4. To Whelan, surveillance may be top-down (conducted by some sort of organizationally central actor), bottom-up (i.e. "sousveillance", inverse surveillance, or surveillance, in which e.g. service providers may engage to protect their interests against users), or networked surveillance (relating to ongoing developments associated with blockchain). "Sousveillance" is a form of "*reflectionism*" invented by Mann for philosophy and procedures as regards using technology to mirror and confront bureaucratic organizations; "reflectionism" thus holds up the mirror and "*asks the question: 'Do you like what you see?' If you do not, then you will know that other approaches by which we integrate society and technology must be considered*". Steve Mann, Jason Nolan, Barry Wellman, Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, Surveillance & Society, 2003, Vol. 1, No. 3, pp. 331-355, at p. 333.

[80] Zuckerman E., The Internet's Original Sin, The Atlantic, 2014, Available at https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/#. As Zuckerman puts it, "[…] *20 years in to the ad-supported web, we can see that our current model is bad, broken, and corrosive. It's time to start paying for privacy, to support services we love, and to abandon those that are free, but sell us —the users and our attention— as the product* […]".

[81] Wally Snyder, Making the Case for Enhanced Advertising Ethics: How a New Way of Thinking About Advertising Ethics May Build Consumer Trust, in Journal of Advertising Research, 2011, Vol. 51, Issue 3, pp. 477-483. Available at http://www.journalofadvertisingresearch.com/content/51/3/477.full.pdf+html.

individuals[82] or target groups, to which personalized ads are addressed[83]. But personal data processing aims not just at commercial targeting (including direct marketing and advertising[84]) or checking and predicting[85] people's characteristics (including trustworthiness, creditworthiness, or identity); it is not just about projecting the "perfect ad"[86] and promoting the appropriate good at the appropriate price[87]; processing also aims to predict criminal behaviors[88] or evaluate the accused before sentencing courts[89].

If the above are not violations of privacy, then what is?

[82] It might be useful to remind that profiling is not new and may be done without modern automated and statistical techniques. Take, for example, practices of profiling by police during stops and searches on the street. Paul De Hert & Hans Lammerant, Predictive profiling and its legal limits: Effectiveness gone forever?, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 145-171, at p. 146 (mentioning that, in general, a profile is a set of characteristics, features, and attributes "*with which a person or a group can be discerned from another person or group*).

[83] See Kati Förster & Ulrike Weish, Advertising Critique: Themes, Actors and Challenges in a Digital Age, in Gabriele Siegert, M. Bjørn von Rimscha, Stephanie Grubenmann (eds), Commercial Communication in the Digital Age, Information or Disinformation?, id, pp. 15-35, at p. 19.

[84] See, for example, recent Youtube's practices with regard to advertising: Chaim Gartenberg, YouTube plans to annoy music listeners into subscribing by playing more ads, 'Frustrate and seduce' users into signing up, The Verge, March 21, 2018, available at https://www.theverge.com/platform/amp/2018/3/21/17147800/youtube-streaming-service-lyor-cohen-ads-music-industry-spotify-free.

[85] Alessandro Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, Vol. 32, Issue 2, April 2016, pp. 238-255, at pp. 239-240 (with further references).

[86] See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, April 2, 2013, at p. 46.

[87] Joseph Turow & Lee McGuigan, Retailing and Social Discrimination: The New Normal?, in Seeta Peña Gangadharan (ed.), Data and Discrimination: Collected Essays, 2014, pp. 27-29. Misuses of an imbalance of power can take several forms and price discrimination is one of them; it enables firms to offer goods or services at different prices to different people, in an effort to extract the maximum price that each consumer is willing to pay. European Data Protection Supervisor, Opinion 7/2015, Meeting the challenges of big data - A call for transparency, user control, data protection by design and accountability, at p. 19.

[88] Anupam Chander, The Racist Algorithm?, Michigan Law Review, 2017, Vol. 115, Issue 6, pp. 1023-1045, at pp. 1026, 1033. Available at https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1657&context=mlr.

[89] See *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), available at https://harvardlawreview.org/2017/03/state-v-loomis/.

Chapter III. The Personal Data Protection Problem

a. Control and Secrecy

The right to the protection of personal data[90], an aspect[91] of the right to privacy[92], is related to personal autonomy and informational self-determination[93], control over data processing[94], and, to some, secrecy[95]. And the most important tool to successfully exercise control is the subject's consent[96], i.e.

[90] The right to the protection of personal data is a fundamental right. Article 8(1-2) of the Charter of Fundamental Rights of the European Union; Article 16(1) of Treaty on the Functioning of the European Union (TFEU).

[91] Maria Bottis, The protection of private life and the European Legislation with regard to Personal Data: Thoughts on the protection of private life in the USA, in M. Stathopoulos, Honorary Volume, Sakkoulas Publications, Greece, 2009, pp. 809-823, at p. 809 (In Greek).

[92] With regard to the right to privacy, Warren and Brandeis were the first to speak of the "*right to be let alone".* S. Warren & L. Brandeis, The right to Privacy, Harvard Law Review, Vol. 4, Ed. 5, 1890, pp. 193-220.

[93] Maria Bottis, Law and information: a "love-hate" relationship, in Maria Bottis (ed.), The history of Information: From papyrus to the electronic document, id, pp. 141-152, at p. 148. The right to informational self-determination was concretized by the German Federal Constitutional Court in 1983 from the basic liberties provided by the German Constitution as protection from the risks of (then) modern data processing. Alexander Roßnagel & Philipp Richter, Big Data and Informational Self-determination. Regulative Approaches in Germany: The Case of Police and Intelligence Agencies, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 261-281, at p. 261 (mentioning that the importance of autonomous decision-making in the disclosure of personal data is protected by informational self-determination).

[94] Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke & Mark Hansen, Self-Surveillance Privacy, Iowa Law Review, 2012, Vol. 97, pp. 809-847, at p. 820; Manon Oostveen & Kristina Irion, The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? University of Amsterdam, Institute for Information Law, Paper No. 2016-06, pp. 1-20, at p. 3 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701, also in Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? 2018, Springer-Verlag Berlin Heidelberg).

[95] Solove sees secrecy as the "*concealment of certain matters from others*". Daniel J. Solove, Conceptualizing Privacy, California Law Review, 2002, Vol. 90, Issue 4, pp. 1087-1156, at pp. 1092, 1106. See also Ann Cavoukian & Don Tapscott, Who Knows: Safeguarding Your Privacy in a Networked World, Random House, 1995. Some regard privacy as a tool that may be used to restrict access to data or to regulate decisions based upon data. See Neil M. Richards & Jonathan H. King, Big Data and The Future for Privacy, id, at p. 8.

[96] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, id, at pp. 260-263; Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review, 2013, Vol. 126, pp. 1880-1903, at p. 1894, mentioning that "[…] *Activities that would otherwise be illegitimate are made legitimate by consent* […]" (available at https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf). See also Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, 01197/11/EN/WP187, at p. 2 ("[…] *If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing* […]").

any freely given[97], specific, informed[98] and unambiguous indication of the data subject's wishes by which she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to her[99].

And firms may process personal data without the subjects' awareness, albeit, they do so with people's given, or "grabbed", consent: under Recital (32) of GDPR, consent can be given by "*ticking a box when visiting an internet website*". This way, a person, who normally never reads the relevant terms of use[100], but generously ticks on boxes, may validly and lawfully give her consent[101] by a mouse-click[102].

---

[97] Consent should not be regarded as freely given, if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (recital (42) of the GDPR). To ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller (recital (43) of the GDPR). Besides, consent is presumed not to be freely given, if it does not allow separate consent to be given to different personal data processing operations (recital (43) of the GDPR). When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Article 7(4) of the GDPR).

[98] For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended (recital (42) of the GDPR).

[99] Article 4(11) of the GDPR.

[100] Zablon Pingo & Bhuva Narayan, When Personal Data Becomes Open Data: An exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy, in Atsuyuki Morishima, Andreas Rauber, Chern Li Liew, Digital Libraries: Knowledge, Information and Data in an Open Access Society (18th International Conference on Asia-Pacific Digital Libraries), ICADL 2016, Springer, pp. 3-9, at p. 4; Susan Gindin, Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears, Northwestern Journal of Technology and Intellectual Property, 2009, Vol. 8, Issue 1, pp. 1-37 (available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1094&context=njtip); Simon Chesterman, Privacy and Our Digital Selves, id, at p. 3 providing further "proof" ("[…] *The British retailer GameStation gave us memorable proof of this one April Fool's Day, when more than 7,000 people clicked "I accept" to terms and conditions that included the surrender of their immortal souls to the company. (The company later rescinded all claims, temporal and spiritual.)* […]"). When users see the term "privacy policy", many of them believe that their data are protected and assume that the webpage will not share their personal information. Turow J., Hoofnagle C. J., Mulligan D. K., Good N. & Grossklags J., The FTC and Consumer Privacy in the Coming Decade, I/S: A Journal of Law and Policy for the Information Society, 2006, Vol. 3, No. 3, pp. 723-749, at p. 724. Even when people read privacy policies, they often do not understand them to make an informed choice. Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, id, at p. 1888.

[101] To some, consent is from the outset pointless, as the very purpose of the processing, for which the individual has to give her consent, has not yet –at the time of "mouse-click"– been decided by the very firm. Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, And Think, id, at pp. 152-153. As authors have commented, some wordings, like "*to personalize customer experience*" or "*to provide personalized offers*"), which are mentioned as "*the purpose of the processing*", are overly broad. Richard Steppe, Online price discrimination and personal data: A General Data Protection Regulation perspective, Computer Law & Security Review, Vol. 33, Issue 6, December 2017, pp. 768-785, at p. 777; Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, 4 April 2008, 00737/EN, WP 148 ("[…] *some purposes, such as 'improvement of the service' or 'the offering of personalised advertising' are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose* […]").

[102] Vranaki questions the validity of the "single-mouse-click-consent", arguing that such an action is an ordinary and mundane deed that cannot fulfill the "*unambiguous indication of the data subject's wishes*"

So, control and self-management is in practice impossible and innumerous jokes on terms of use[103] can prove this. The choice to disclose personal data is an illusion, as one has no choice to opt-out of profiling by firms, of whose existence she is unaware. Besides, opting-out of the alleged[104] –firms' and governments'– surveillance[105] would mean opting-out of society[106]. Indeed, if one truly wished privacy, then she would need to keep her data to herself; use no credit cards, no Internet, no phone; have no bank account, no job; and, in general, do not do "*anything that would create a record*"[107]. But would one really wish to opt-out from the 21st century?

Besides, firms may further process personal data to render re-identification of the individual impossible[108]. Anonymization, i.e. further data processing[109], comes after data collection –and after having obtained the individuals' consent. Anonymized, ex-personal, data can be "freely" used, since principles of data protection do not apply to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[110].

---

by which the individual has to signify agreement to the processing of her personal data. Asma Vranaki, Social Networking Site Regulation: Facebook, Online Behavioral Advertising, Power and Data Protection Laws, Rutgers Computer & Technology Law Journal, Queen Mary School of Law Legal Studies Research Paper No. 221/2016, pp. 1-30, at p. 29 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731159).

[103] Simon Chesterman, Privacy and Our Digital Selves, id; Alexis Madrigal, Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days, The Atlantic (Mar. 1, 2012), available at https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[104] As some have put it, technologically enhanced surveillance is changing policing into an "*almost entirely informationalised activity*". Aleš Završnik, Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?, in Journal of Contemporary European Research, 2013, Vol. 9, Issue 1, pp. 182-202, at p. 192. Available at https://www.jcer.net/index.php/jcer/article/view/452/394. See also Rosamunde van Brakel, Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 117-141, at p. 118 (defining surveillance as the systematic or targeted collection and processing of data that are used to make predictions about future harm on the basis of profiles with the main goal of intervening before harm is done). To Brakel, the pre-emptive society is about imaginary surveillance control, which is "*a fantastic dream of seeing everything capable of being seen, recording every fact capable of being recorded, and accomplishing these things, whenever and wherever possible, prior to the event itself* […] *it circulates as an effective mechanism in the technical evolution of control in postindustrial societies*" (Rosamunde van Brakel, Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing, id, at p. 117).

[105] See, amongst others, Parker Higgins, Big Brother Is Listening: Users Need the Ability to Teach Smart TVs New Lessons, The Electronic Frontier Foundation, Feb. 11, 2015, available at https://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons.

[106] See, in general, Julia Angwin, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance, 2015, S. Martin's Griffin Edition.

[107] Daniel J. Solove, Nothing to Hide, id, at p. 110.

[108] W. Kuan Hon, Christopher Millard & Ian Walden, The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, International Data Privacy Law, 2011, Vol. 1, No. 4, pp. 211-228; Sophie Stalla-Bourdillon & Alison Knight, Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization, and Personal Data, Wisconsin International Law Journal, 2017, Vol. 34, No. 2, pp. 284-322.

[109] See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, 0829/14/EN, WP216, at p. 3.

[110] See recital (26) of GDPR.

But in the age of Big Data the "anonymized data subject" may be in any case identifiable[111] and, as many authors argue, there is no manner in which to render personal data anonymous[112]. Failure to anonymize personal data is due to collection and correlation[113] of a huge volume of data, derived from multiple sources, and, hence, the capacity to draw countless conclusions about a person. Anonymization, a temporary state[114] in the arena of Big Data, can only be achieved in Small Data environments[115]. With click-stream profiling and Deep Packet Inspection (DPI) that have become increasingly commonplace[116] it is extremely difficult for end-users to avoid being re-identified[117].

---

[111] Tobias M. Scholz, Big Data in Organizations and the Role of Human Resource Management, id, at p. 35 (with further references); Bruce Schneier, Data and Goliath, id, at pp. 50-53.

[112] Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of anonymization, UCLA Law Review, 2010, Vol. 57, pp. 1701-1777 (University of Colorado Law Legal Studies Research Paper No. 9-12); Latanya Sweeney, Simple demographics often identify people uniquely, Carnegie Mellon University, 2000, Data Privacy Working Paper No. 3, pp. 1-34 (available at https://dataprivacylab.org/projects/identifiability/paper1.pdf); Philippe Golle, Revisiting the uniqueness of simple demographics in the US population, 5th ACM Workshop on Privacy in the Electronic Society (WPES'06), Alexandria, Virginia, USA, October 30, 2006, pp. 77-80; Melissa Gymrek, Amy L. McGuire, David Golan, Eran Halperin, Yaniv Erlich, Identifying personal genomes by surname inference, Science, 2013, Vol. 339, Issue 6117, pp. 321-324 (available at http://science.sciencemag.org/content/339/6117/321/tab-pdf); John Bohannon, Genealogy databases enable naming of anonymous DNA donors, Science, 2013, Vol. 339, Issue 6117, p. 262; Arvind Narayanan & Vitaly Shmatikov, Robust de-anonymization of large sparse datasets, IEEE Symposium on Security and Privacy (May 18-22, 2008, Oakland, CA, USA), pp. 111-125 (available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4531148).

[113] "[…] *Whether born analog or digital, data* […] [are] *being reused and combined with other data in ways never before thought possible, including for uses that go beyond the intent motivating initial collection* […]". John Podesta, Penny Pritzker, Ernest J. Moniz, John Holdren, Jeffrey Zients, Big Data: Seizing Opportunities, Preserving Values, id, at p. 54; Alexander Roßnagel & Philipp Richter, Big Data and Informational Self-determination. Regulative Approaches in Germany: The Case of Police and Intelligence Agencies, id, at p. 266 (arguing that the very concept of Big Data is to retain data for unspecified purposes and to combine them freely and repeatedly).

[114] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, id, at p. 257; Mario Viola de Azevedo Cunha, Review of the Data Protection Directive: Is There Need (and Room) For a New Concept of Personal Data?, in S. Gutwirth et al. (eds), European Data Protection: In Good Health?, 2012, Springer, pp. 267-284, at p. 270.

[115] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, And Think, id, at p. 154.

[116] Deep packet inspection allows operators to scan the payload (or content) of IP packets as well as the header; DPI systems use regular expressions to define patterns of interest in network data streams. Ralf Bendrath & Milton Mueller, The End of the Net as We Know it? Deep Packet Inspection and Internet Governance, New Media & Society, 2011, Vol. 13, No. 7, pp. 1142-1160; Robert Todd & Graham Collins, The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat, Georgia Law Review, 2010, Vol. 44, pp. 545-579 (at p. 550, mentioning that DPI technology has been described as part of focus of congressional hearings on Internet privacy standards).

[117] Max Van Kleek, Daniel A. Smith, Dave Murray-Rust, Amy Guy, Kieron O'Hara, Laura Dragan, Nigel R. Shadbolt, Social Personal Data Stores: The Nuclei of Decentralised Social Machines, World Wide Web '15 Companion Proceedings of the 24th International Conference on World Wide Web, Florence, Italy, May 18-22, 2015, ACM, New York, USA, pp. 1155-1160, at p. 1157. See also Teaching Privacy website, Principles: There is no anonymity on the Internet, available at http://www.teachingprivacy.org/theres-no-anonymity/ (mentioning that "[…] *It is virtually impossible to remain anonymous on the Internet* […] *some details of your device's setup are communicated to your Internet service provider, and often to the site or service you are using* […] *your IP address is always transmitted* […] *details can be combined together to serve as a unique identifier* […]"). To

So, one could fairly argue that an individual is not capable of controlling when and by whom the thoughts in her head will be experienced by someone other than themselves; one is not capable of keeping the contents of her consciousness (anonymous or) secret[118]. Such lack of secrecy and absence of control[119] can be regarded as two important aspects of the personal data protection problem.

b. Value

Personal data do have an important societal[120] and economic[121] value[122]. And the notion that persons are the producers, the "creators", and the owners of their digital information and activities[123] raises the question: How could value[124] be equitably distributed[125]?

---

some, the impossibility to remain anonymous relates to "surveillance capitalism". Shoshana Zuboff, Big other: Surveillance capitalism and the prospects of an information civilization, Journal of Information Technology, 2015, Vol. 30, pp. 75-89. To others, this impossibility is due to the success of Web 2.0 technologies. Tim O'Reilly, What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, Communications and Strategies, Vol. 65, 1st Q. 2007, pp. 17-37.

[118] Some authors arguing for the social aspect of privacy, have defined people's –privacy and– ownership of their thoughts as the ability to see themselves as autonomous, to learn that they are capable of controlling when and by whom the thoughts in their head will be experienced by someone other than themselves, and to learn that they are entitled to such control and that they will not be forced to reveal the contents of their consciousness even if they put such contents on paper. Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, Philosophy & Public Affairs, 1976, Vol. 6, No. 1, pp. 26-44, at p. 43. Available at https://www.jstor.org/stable/pdf/2265060.pdf?refreqid=excelsior%3Accf8fd81d9b68e61247344eff393e67f.

[119] Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, GW Law Faculty Publications & Other Works Faculty Scholarship, Stanford Law Review, 2001, Vol. 53, pp. 1393-1462, at pp. 1418-1419, 1422 (referring to databases, which subject personal data to the bureaucratic process, resulting in a lack of meaningful participation in decisions about our information; it is a problem, implicating "[…] *the type of society we are becoming, the way we think, our place in the larger social order, and our ability to exercise meaningful control over our lives* […]"). Available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2077&context=faculty_publications.

[120] Indeed, by processing personal data several economically and socially useful purposes have been achieved in several fields, including health care, education, commerce, crime detection or terrorism prevention. Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at pp. 226-230; Bartha Maria Knoppers & Adrian Mark Thorogood, Ethics and Big Data in health, Big data acquisition and analysis, Current Opinion in Systems Biology, 2017, Vol. 4, pp. 53-57. As some have argued, the social nature of data presents questions of social justice, which can be defined as the central ethical judgment regarding the effects of society on the situation of social entities. Jeffrey Alan Johnson, From Open Data to Information Justice, Ethics and Information Technology, December 2014, Vol. 16, Issue 4, pp. 263–274, at p. 264.

[121] Klaus Schwab, Alan Marcus, Justin Rico Oyola, William Hoffman, Michele Luz, Personal Data: The Emergence of a New Asset Class, 2011, World Economic Forum, available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[122] As some have put it, personal data are valuable to firms; without our information they would become bankrupt. Finn Brunton, Helen Nissenbaum, Obfuscation: A User's Guide for Privacy and Protest, MIT Press Scholarship Online: September 2016, at p. 50. DOI:10.7551/mitpress/9780262029735.001.0001. Available at http://mitpress.universitypressscholarship.com/view/10.7551/mitpress/9780262029735.001.0001/upso-9780262029735. The economic value of personal data has been calculated by economists, consulting groups or even media. OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, 2013, No. 220, OECD Publishing,

Indeed, economists attribute injustice, bureaucracy, and societal inefficiency to asymmetric data flows, meaning the situation in which one person or group knows something that others do not[126]; uneven

Paris (available at https://read.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en#page4); Chirita D. Anca, The Rise of Big Data and the Loss of Privacy, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach? Bakhoum, M., Gallego Conde, B., Mackenordt, M.-O. & Surblyte, G. (eds) Berlin Heidelberg, Springer, 2018 (forthcoming), Durham Law School Research Paper (2016), pp. 1-33, at p. 11 (available at https://ssrn.com/abstract=2795992); European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, at p. 9 (available at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf); Boston Consulting Group, The Value of our Digital Identity, November 2012, Liberty Press (available at http://www.cil.cnrs.fr/CIL/IMG/pdf/The-Value-of-Our-Digital-Identity-2.pdf). See also the Financial Times' "personal data's value calculator": http://ig.ft.com/how-much-is-your-personal-data-worth/; Researches in press articles: Telegraph: http://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html; The Guardian: https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth.

[123] To some, our names, our addresses, and our personal transactions are valuable information assets worthy of recognition that we have property rights in them. Richard Spinello, Property Rights in Genetic Information, in Herman Tavani (ed.), Ethics, Computing, and Genomics, Jones & Bartlett Publishers, 2006, pp. 213-234, at p. 217 (citing Anne Wells Branscomb, Who Owns Information? From Privacy to Public Access, HarperCollins, New York, 1994).

[124] As some argue, data concerning age may be worth less than sensitive information relating to health that may be worth about 26 cents per person. Gianclaudio Malgieri & Bart Custers, Pricing Privacy: The Right to Know the Value Of Your Personal Data, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, Issue 2, April 2018, pp. 289-303, at p. 294, mentioning that the total value of such information may be less than a dollar per person, albeit, each person provides her data constantly and on a daily basis, while one may provide same data to multiple firms. See also at p. 300, where the authors argue for people's right to know the value of their personal data; the provision of this information could follow the reasoning of other information duties for data controllers (Articles 13 and 14 of the GDPR).

[125] Klaus Schwab, Alan Marcus, Justin Rico Oyola, William Hoffman, Michele Luz, Personal Data: The Emergence of a New Asset Class, id, at p. 17.

[126] Xiaodong Jiang, Jason I. Hong, and James A. Landay, Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing, in G. Borriello and L.E. Holmquist (eds), UbiComp 2002, LNCS 2498, Springer-Verlag Berlin Heidelberg, pp. 176-193, at p. 179 (available at https://link.springer.com/content/pdf/10.1007%2F3-540-45809-3.pdf), defining "environments with asymmetric information" as situations in which some actors hold private information that is relevant to anyone. See also at p. 176, where the authors regard privacy as "[…] *an interaction, in which the information rights of different parties collide* […] *the issue is of control over information flow by parties that have different preferences over 'information permeability'* […]".

knowledge is put right at the top, when experts list the causes of "market failure"[127] (i.e. things that make simple markets handle problems poorly)[128].

Control over data processing, as it is mainly exercised by firms, enables the controlling party to know[129]; and knowledge brings power[130]. But when too much power is accumulated in the hands of the few (and stronger), equality may be threatened[131].

This unequal distribution of personal data's value is another crucial aspect of the personal data protection problem.

c. Otherness

When power is accumulated in private hands, the fundamental right to non-discrimination may be threatened[132]. The potential of machines to create discriminatory biases[133] and unfair results or

[127] To economists, a market failure exists when market prices cannot reach "*a self-sustaining equilibrium*". Eli Noam, Market Failure in the Media Sector, The Financial Times online, February 16, 2004 (available at http://www.citi.columbia.edu/elinoam/articles/Market_Failure_in_MediaSector.pdf). See also Eli Noam, Privacy and Self-Regulation: Markets for Electronic Privacy, in Privacy And Self-Regulation In The Information Age, U.S. Department Of Commerce, Washington, D.C., June, 1997 (short version available at http://www.citi.columbia.edu/elinoam/articles/priv_self.htm, mentioning that for privacy transactions to occur, there are several prerequisites, including –amongst others– symmetry of information among the transacting parties and no market failure, i.e. no growing instability in the market).

[128] David Brin, The Transparent Society, id, at p. 24. As Brin puts it, if transparency is a requisite condition in science, democracy, and free markets, it is no surprise that economists find openness appealing.

[129] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, And Think, id, at pp. 50-61.

[130] Aaron Swartz, Guerilla Open Access Manifesto, 2008, (available at https://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, id, at pp. 1402-1407, arguing that personal data processing is valuable as it promotes greater scientific and commercial understanding of individual behavior and desires; see also at p. 1408, mentioning that if data constructs truth, it is then possible to attain power.

[131] See Peter Ulrich, Integrative Economic Ethics: Foundations of a Civilized Market Economy, 2008, Cambridge University Press (available at http://www.villafane.com/wp-content/uploads/2015/11/Cap-1_Integrative-Economic-Ethics_Peter-Ulrich.pdf), at p. 228, mentioning that the moral equality of all human beings implies in its essence their equal freedom and "inviolability"; freedom can thus be only justified as general freedom, as the greatest possible equal freedom of all persons – anything else would be arbitrary freedom, which would mean by "freedom" merely the right of the stronger to an undisturbed and unlimited assertion of their own interests without consideration of the equally legitimate claims to freedom of others.

[132] Under Article 21(1-2) of the Charter of Fundamental Rights of the European Union "[…] *Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited* […] *Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited* […]".

[133] To Brakel, algorithmic discrimination may be the result of three types of bias creep: bias that unintentionally creeps into the labelling of examples or the rules that are coded into the algorithm;

exacerbate inequality has been widely acknowledged[134]. People may enjoy the right to obtain details of any personal data used for profiling[135], albeit there is no right to an explanation of a particular decision[136]. This way, one may ignore ways in which information existing about her is created or modified[137].

In particular, by linking datasets, even seemingly neutral data, such as postcodes, can lead to discrimination[138] based on sensitive information[139]. Powerful algorithms make automated decisions and score individuals to statistically characterize everything[140]; from one's ability to pay to whether a prisoner is eligible for parole[141]. Such scores may be used to influence a person's opportunities to, e.g., find housing or a job or estimate health[142].

---

biased assumptions that are baked into the data; and bias creep that occurs due to technical defects, faults, and bugs in the system. Rosamunde van Brakel, Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing, id, at p. 125.

[134] Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, Kate Crawford, AI Now 2017 Report, Andrew Selbst, Solon Barocas (eds), AI Now Institute, at p. 13. Available at https://ainowinstitute.org/AI_Now_2017_Report.pdf.

[135] Article 15 of the GDPR.

[136] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on October 3, 2017, at p. 24, where it is also mentioned that simple ways should be found to tell the data subject about the rationale behind or the criteria relied on in reaching the decision. A mathematical explanation about how algorithms work should also be provided to allow experts to verify how the decision-making process works. Article 29 Data Protection Working Party, id, at pp. 14, 29.

[137] Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, Volume 34, Issue 3, June 2018, pp. 436-449, at p. 439. Wachter argues that when a person is unaware that her devices generate information about her, she lacks the ability to incorporate this information into her self-constructed identity, and to view herself as others view her. See also Luciano Floridi, The Informational Nature of Personal Identity, Minds and Machines, 2011, Vol. 21, Issue 4, pp. 549-566, at p. 549.

[138] Salvatore Ruggieri, Dino Pedreschi, Franco Turini, Data Mining for Discrimination Discovery, ACM Transactions on Knowledge Discovery from Data, Vol. 4, No. 2, May 2010, pp. 9-49; Solon Barocas & Andrew Selbst, Big Data's Disparate Impact, 2016, California Law Review, Vol. 104, pp. 671-732, available at https://ssrn.com/abstract=2477899 or http://dx.doi.org/10.2139/ssrn.2477899. As reported some years ago, business models and strategies built around collection and use of personal data raise very important issues with regard to discrimination. See John Podesta, Penny Pritzker, Ernest J. Moniz, John Holdren, Jeffrey Zients, Big Data: Seizing Opportunities, Preserving Values, id, at p. 45.

[139] Bart W. Schermer, The limits of privacy in automated profiling and data mining, Computer Law & Security Review, Vol. 27, Issue 1, February 2011, pp. 45-52, at p. 47.

[140] Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information, id, at pp. 8, 30, 34; Cathy O' Neil, Weapons of Math Destruction, id.

[141] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, Machine Bias, There's software used across the country to predict future criminals. And it's biased against blacks, ProPublica, May 23, 2016. Available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also Rosamunde van Brakel & Paul De Hert, Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies, 2011, Cahiers Politiestudies, Vol. 3:20, pp. 163-192, at p. 174, available at http://www.vub.ac.be/LSTS/pub/Dehert/378.pdf.

[142] Pam Dixon and Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, World Privacy Forum, April 2, 2014, at pp. 13-15. Available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

Namely, as regards advertising techniques, innumerous targeting settings are set to exclude more and more individuals and reach a perfect audience[143]. This way, job seekers may be excluded from seeing a job advertisement[144], and this threatens equality, whose principle demands that every individual should have the same opportunities –including access to employment[145].

Online advertising[146] differs from traditional techniques; human input is used to run an ad campaign and the audience can thus be manipulated precisely, rather than generally. Hence, the effectiveness of advertising increases, since personalized ads reach the right individual at the right time[147]. So, attention is drawn to reaching the right people and showing them what they wish to see.

In fact, a firm may target its ads based on location (e.g. zip code, city, or country), age, gender, demographics (e.g. income, job title, employer name, language, relationship status, education, financial or parental status), interests, behaviors (such as online shopping or travel habits), or connections (meaning people connected to one's page, app, and so forth)[148]. The above targeting may be conducted by humans or by an automated process; when Artificial Intelligence[149] (AI) is used to tailor automated ads, it makes targeting decisions and examines results based on pre-programmed and self-learned strategies.

And the way systems learn how to make decisions is machine learning[150], which makes AI better capable of making the right decision; the longer it learns the more efficient and higher the quality of its

[143] Amit Datta, Michael Carl Tschantz, Anupam Datta, Automated Experiments on Ad Privacy Settings, A Tale of Opacity, Choice, and Discrimination, in Proceedings on Privacy Enhancing Technologies (PoPETs), 2015, De Gruyter Open. Extended version available at https://arxiv.org/pdf/1408.6491.pdf.

[144] Paul Post and Rikki Holtmaat, A False Start: Discrimination in Job Advertisements, European Gender Equality Law Review – No. 1/2014, at p. 12. Available at https://openaccess.leidenuniv.nl/bitstream/handle/1887/35024/EGELR%202014-2%20-%20PP%20%26%20RH%20-%20A%20False%20Start.%20Discrimination%20in%20Job%20Advertisements.pdf?sequence=1.

[145] Richard J. Arneson, Equality of Opportunity: Derivative Not Fundamental, Journal of Social Philosophy, Wiley Periodicals, Inc., Vol. 44, No. 4, Winter 2013, pp. 316-330, available at https://onlinelibrary.wiley.com/doi/pdf/10.1111/josp.12036; Richard Arneson, Egalitarianism, The Stanford Encyclopedia of Philosophy, Summer 2013 Edition, Edward N. Zalta (ed.), available at https://plato.stanford.edu/entries/egalitarianism/.

[146] See, for example, Facebook Ads: https://www.facebook.com/business/products/ads.

[147] Alexander Bleier, Maik Eisenbeiss, Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where, Marketing Science, 2015, Vol. 34, No. 5, pp. 669-688, at p. 669.

[148] See Kane Jamison, The Big Damn Guide to Facebook Ad Targeting, available at https://www.contentharmony.com/blog/facebook-ad-targeting/#facebook-ad-targeting-overview.

[149] Artificial Intelligence (AI) could be defined as any system or device that perceives its environment and undertakes actions that maximize its chance of success at some goal. See definitions of AI in Stuart Russell, Peter Norvig, Artificial Intelligence, A Modern Approach, 2nd Ed., 2003, 1995 by Pearson Education, Inc. Pearson Education, Inc., at pp. 2-5. Available at http://www.eng.uerj.br/~fariasol/disciplinas/Topicos_B/AGENTS/books/Stuart%20Russell,%20Peter%20Norvig-Artificial%20Intelligence_%20A%20Modern%20Approach-Prentice%20Hall%20(2002)-2nd-ed.pdf. See also Nick Bostrom, Superintelligence: Paths, Dangers, Strategies, Oxford University Press, 2014.

[150] Machine learning focuses on ways to construct a system that automatically improves through experience and on finding the fundamental statistical, computational, information theoretic laws that govern all learning systems. M. I. Jordan, T. M. Mitchell, Machine learning: Trends, perspectives, and prospects, Science, 2015, Vol. 349, Issue 6245, pp. 255-260, DOI: 10.1126/science.aaa8415, at p. 255. Available at http://science.sciencemag.org/content/349/6245/255.full. To some, machine learning may

decisions. For instance, with regard to job ads, the system will learn the targeting settings that are the most effective for a job. Since the algorithm looks for statistical correlations of data, rather than understanding cause-and-effect relationships[151], patterns may seem random to humans, to whom settings would never have occurred. Namely, AI may find that female individuals perform worse than males when undertaking a specific task. So, it can exclude females and show the (e.g. job) ad to a male audience.

An "algorithmic governmentality" aims to bring order to the chaos of the online world[152] and make information easily manageable for the everyday user. But when systems aim at "*n=all*"[153] and rely on data, rather than users' internal motivations[154], conclusions are invisible to humans[155]. Hence, any individual, without being party to any contract and without being related –in any way– to a firm, may be affected and influenced.

It seems that data distribution has turned the "*quantified self*", i.e. any individual engaged in self-tracking of any kind of biological, physical, behavioral, or environmental information[156], into a "*quantified otherness*", where people are approached, influenced, and affected[157] through data[158].

And this otherness is another important aspect of the personal data protection problem.

---

refer to techniques, methods, and processes for analyzing datasets to provide useful summaries or using models developed on sample data to make predictions. Seda Gürses & Bart Preneel, Cryptology and privacy in the context of big data, id, at p. 51 (see also at p. 52, mentioning that since machine learning could be applied to the user data 'troves' to scale and shape services and profile users, concerns about discrimination, unfair treatment, and human experimentation are amplified). See also proposals on machine learning systems designing to limit discrimination in Michael Veale & Reuben Binns, Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data, Big Data & Society, 2017, Vol. 4, Issue 2 (available at http://journals.sagepub.com/doi/abs/10.1177/2053951717743530). For machine learning systems, see, in general, Trevor Hastie, Robert Tibshirani & Jerome Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Series in Statistics, 2nd ed., 2009. Available at https://web.stanford.edu/~hastie/Papers/ESLII.pdf.

[151] Allan G. King & Marko Mrkonich, "Big Data" and the Risk of Employment Discrimination, Oklahoma Law Review, 2016, Vol. 68, Issue 3, pp. 555-584, at p. 555, available at https://digitalcommons.law.ou.edu/olr/vol68/iss3/3/; Viktor Mayer-Schonberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, And Think, id, at p. 68 mentioning that "[…] *Causality won't be discarded, but it is being knocked off its pedestal as the primary fountain of meaning. Big data turbocharges non-causal analyses, often replacing causal investigations* […]".

[152] Rouvroy uses the term "algorithmic governmentality" to refer to new regimes of power brought by the computational turn and the prevalence of algorithms in daily life. Antoinette Rouvroy, The end(s) of critique: data-behaviourism vs. due-process, in Privacy, Due Process and the Computational Turn, Mireille Hildebrandt, Ekatarina De Vries (eds), Routledge, 2012, pp. 143-167, at p. 151.

[153] Rob Kitchin, The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences, 2014, Sage Publications, London, at p. 72, mentioning that big data is "[…] *exhaustive in scope, striving to capture entire populations or systems (n=all)* […]".

[154] Antoinette Rouvroy, The end(s) of critique: data-behaviourism vs. due-process, id, at p. 143.

[155] Mireille Hildebrandt, Bert-Jaap Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, The Modern Law Review, Vol. 73, Issue 3, May 2010, pp. 428-460, at pp. 429-432. Available at https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1468-2230.2010.00806.x.

[156] Melanie Swan, The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery, Big Data, 2013, Vol. 1, Issue 2, pp. 85-99, at pp. 85-86.

[157] Namely, as regards (unawareness of) people affected by scoring, see Pam Dixon and Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, id.

[158] Katleen Gabriels, 'I keep a close watch on this child of mine': A moral critique of other-tracking apps, Ethics & Information Technology, 2016, Vol. 18, No. 3, pp. 175-184, at p. 176.

Chapter IV. A Property-Like Approach

a. The Notion of Ownership

Property rights[159] are the rights of ownership, the notion of which includes the right to possess; the right to use; the right to manage; the right to the income; the right to destroy; the right to modify; the right to alienate or to abandon ownership; the right to transmit; the right to security; the prohibition of harmful use; the absence of term; liability to execution; and residuary rules that govern the reversion to another, if any, of ownership rights which have expired or been abandoned[160].

Some or all of the above elements can be detected in the notion of personal data possession.

In particular, the right to possess means that a person has the right to exclusive control of the thing[161], which, in case of intangible items, may be understood metaphorically. Similarly, the principles of personal data protection laws include respect for personal autonomy, safeguarding rights to informational self-determination, and, ultimately, control over the processing of such data[162].

The right to use, to personal enjoyment of the benefits of the thing, other than those of management and income[163], may also be detected, as an individual has the right to use and enjoy benefits deriving from her personal data (e.g. e-mail, IP address, or cookies)[164]. Besides, by using cookies, firms offer "the best experience" and, thus, consumers enjoy the "benefits of the thing"[165].

The right to manage, to decide how and by whom a thing should be used[166], can also be found in the concept of data possession; the tool to successfully exercise control is the subject's consent[167]. So, the

[159] The typical right to a thing (or real right) is the property right; traditional science of law defines it as the exclusive dominion of a person over a thing and, therefore, distinguishes it from the right to claim that is the basis only of personal legal relations. Hans Kelsen, Pure Theory of Law, Max Knight (translation), The Lawbook Exchange, Ltd., Clark, New Jersey, 2005, at pp. 130-131.

[160] In every case, to have a property right in a thing is to have a bundle of rights that defines a form of ownership. Lawrence C. Becker, The Moral Basis of Property Rights, in Nomos XXII: Property, edited by J. Roland Pennock and John W. Chapman, pp. 187-220, New York, New York University Press, 1980, Hollins Digital Commons, Web, at pp. 189-191. Available at https://digitalcommons.hollins.edu/cgi/viewcontent.cgi?article=1020&context=philfac.

[161] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[162] Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke & Mark Hansen, Self-Surveillance Privacy, id, at p. 820; Manon Oostveen & Kristina Irion, The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?, id, at p. 3.

[163] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[164] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, id; Opinion 1/2008 on data protection issues related to search engines, id.

[165] Aaron Schmidt, The user experience, Data-driven design, Library Journal, April 1, 2016, Vol.141, No. 6, at p.26; Caroline Bader, Eva-Louise Castefelt, Louise Gunnarsson, The Recipe for Cookies: A studies about cookies & the GDPR-law, Högskolan i Borås, Akademin för bibliotek, information, pedagogik och IT, 2018 Uppsala University Library (available at http://hb.diva-portal.org/smash/get/diva2:1219987/FULLTEXT01.pdf).

[166] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[167] Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, id, at p. 1894.

data subject has the right to manage her information and decide how and by whom her information should be used[168].

The right to the income –that is to the benefits deriving from personal use of an item and allowing others to use it[169]– is a right, for which, in case of personal data, authors have been arguing, supporting that users should have the right to know the value of their data[170] and participate in profits[171]. Besides, consumers enjoy some "benefits" deriving from allowing firms to use their data, with which innumerous "free" digital services are paid for.

The right to erasure[172], to be forgotten[173], enabling the individual to obtain from the controller the erasure of personal data[174], resembles the right of the owner to destroy a thing[175]. The right to modify the thing, to effect changes less extensive than annihilation, may also be found in the notion of personal data possession, as the individual has the right to modify her e-mail address or her name. The right to alienate or to abandon ownership reminds of cases, where the European Court of Human Rights held

[168] Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, id, at p. 43.

[169] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[170] Gianclaudio Malgieri & Bart Custers, Pricing Privacy: The Right to Know the Value of Your Personal Data, id.

[171] Rachana Nget, Yang Cao, Masatoshi Yoshikawa, How to Balance Privacy and Money through Pricing Mechanism in Personal Data Market, SIGIR 2017 eCom, August 2017, Tokyo, JAPAN, available at https://arxiv.org/pdf/1705.02982.pdf (proposing a "practical" personal data trading framework to strike a balance between money and privacy).

[172] The right to erasure is not new, as obligations to delete personal data were also provided under the Data Protection Directive. Take, for example, Articles 6(1)(e) and 12(b) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter referred to as the "Data Protection Directive".

[173] Scholars have been discussing the right to be forgotten since the 1990s. DH Flaherty, Controlling Surveillance: Can Privacy Protection Be Made Effective? in PE Agre and M Rotenberg (eds), Technology and Privacy: The New Landscape, Cambridge, MA/London: The MIT Press, 1998, pp. 167-192, at p. 172. Although the right to be forgotten has been established by the GDPR as a right, some scholars have argued that it could be framed as an ethical or social value or as a virtue or policy aim. J. F. Blanchette and D.G. Johnson, Data Retention and the Panoptic Society: The Social benefits of Forgetfulness, The Information Society, 2002, Vol. 18, pp. 33-45, available at https://pdfs.semanticscholar.org/f17f/fed4d7cd491796e7384f66204a11010ab0b0.pdf; M. Dodge and R. Kitchin, Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting, Environment and Planning B: Planning and Design, 2007, Vol. 34, pp. 431-445, available at http://personalpages.manchester.ac.uk/staff/m.dodge/cv_files/epb_ethics_of_forgetting.pdf.

[174] See Article 17(1) of the GDPR.

[175] Nadezhda Purtova, Property rights in personal data: A European perspective, 2011, Oisterwijk, BOXPress, BV, available at https://pure.uvt.nl/ws/files/1312691/Purtova_property16-02-2011.pdf, at p. 56 (mentioning that "[…] *by stating that some 'thing' is 'mine', a layperson implies that he can do what he pleases with it, including destroying or selling it* […]"); Lawrence C. Becker, The Moral Basis of Property Rights, id, at p. 191 (who defines the right, or liberty, to destroy or consume as the right to "*annihilate the thing*"); Bert-Jaap Koops, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice (December 20, 2011), SCRIPTed, Vol. 8, No. 3, pp. 229-256, Tilburg Law School Research Paper No. 08/2012. Available at SSRN: https://ssrn.com/abstract=1986719 or http://dx.doi.org/10.2139/ssrn.1986719, at p. 247 ("[…] *However, if a right to be forgotten is cast in the form of a property right for data subjects to delete (abusus), this being the strongest property stick, then likely the entire bundle of sticks would have to be allocated to data subjects, which seems a bridge or two too far* […]").

that an individual may consent to waiving a fundamental right[176]. And the need for free flow of personal data, illustrating a utilitarian approach, enables an individual to transmit her data[177]; this resembles the right to transmit, to devise or bequeath a thing[178].

Besides, personal data should be processed in a manner that ensures appropriate security, meaning protection against unauthorized or unlawful processing, accidental loss, destruction or damage[179]. Similarly, in the case of ownership there is the right to security, to immunity from expropriation, and the prohibition of harmful use, meaning one's duty to forebear from using the thing in ways harmful to oneself or others[180].

But ownership lasts forever, which is not the case as regards personal data protection. However, if such data were examined in a *sui generis* right of a database, then it could be argued that this protection may last for an eternity[181], albeit, in favor of the database maker.

Liability to execution, meaning to have the thing taken away as payment for a debt[182], can also be found in data possession; there have been cases, where firms decided to have their consumers' data taken away as payment for a debt or as a way to silence creditors[183].

Finally, residuary rules govern the reversion to another, if any, of ownership rights, which have expired or been abandoned[184]. Such rules are, for example, those that determine the disposition of property left by intestate deaths. And, interestingly, under some national laws, personal data enjoy protection after one's death[185].

---

[176] See *Deweer/Belgium*, ECHR, 27 February 1980, A35, paragraphs 48-54; *De Wilde, Ooms, Versyp/Belgium*, ECHR, 18 June 1971, A12 paragraphs 64-65.

[177] See Article 20(1) of the GDPR.

[178] A. M. Honoré, Ownership, in A. G. Guest (ed.), Oxford essays in jurisprudence, a collaborative work, London, Oxford University Press, 1961, pp. 107-147.

[179] Article 5(1)(f) of the GDPR.

[180] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[181] Mark Davison, Database Protection: The Commodification of Information, in Lucie Guibault and P. Bernt Hugenholtz (eds), The Future of the Public Domain, id, pp. 167-189, at pp. 169, 187, who mentions that the greatest possible period of protection was conferred on the least creative element of intellectual property. See also James Boyle, Foreword: The Opposite of Property? Law and Contemporary Problems, Vol. 66, pp. 1-32 (Winter 2003), at p. 25 (available at https://scholarship.law.duke.edu/lcp/vol66/iss1/1), mentioning that "[…] *a so-called 'database right'* […] *allows ownership of unoriginal compilations of factual data* […]".

[182] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[183] See Lori Enos, Deal Afoot to Destroy Toysmart Database, E-commerce Times, January 10, 2001. Available at https://www.ecommercetimes.com/story/6607.html; Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at p. 228.

[184] Lawrence C. Becker, The Moral Basis of Property Rights, id.

[185] The European Data Protection Directive did not mention anything about the data of the deceased and, hence, some European Member States decided to protect them. For instance, under Bulgarian law, in case a natural person dies, her rights of access may be exercised by heirs, who are enabled, amongst others, to request, at any time and free of charge, from the personal data controller a confirmation as to whether or not data relating to the deceased are being processed, information as to the purposes of such processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. See Article 28(3) of the Bulgarian Law For Protection Of Personal Data (Prom. SG. 1/4 Jan 2002, amend. SG. 70/10 Aug 2004, amend. SG. 93/19 Oct 2004, amend. SG. 43/20 May 2005,

So, the notion of ownership and the concept of personal data possession do share some common features. But could property rights[186] be introduced[187] to address –at least some aspects of– the personal data protection problem?

b. Personal Data as Intellectual Property

Firms, behaving as owners of information[188], impose the conditions under which data may be shared[189]; treating data as a commodity[190] and as an asset[191], they process or sell[192] them, and, in general, they

---

amend. SG. 103/23 Dec 2005, amend. SG. 30/11 Apr 2006, amend. SG. 91/10 Nov 2006, amend. SG. 57/13 Jul 2007, amend. SG. 42/5 Jun 2009, amend. SG. 94/30 Nov 2010, amend. SG. 97/10 Dec 2010, amend. SG. 39/20 May 2011, amend. SG. 81/18 Oct 2011, amend. SG. 105/29 Dec 2011). Available at http://legislationline.org/topics/country/39/topic/3. Under the Estonian Personal Data Protection Act (passed 15.02.2007, RT I 2007, 24, 127, Entry into force 01.01.2008, available at https://www.riigiteataja.ee/en/eli/512112013011/consolide), the consent of a data subject remains valid during the lifetime of the data subject and for thirty years after the death of the data subject, unless the individual has decided otherwise. Besides, under the above Act, processing of personal data relating to the deceased is permitted only with the written consent of the successor, spouse, descendant or ascendant, brother or sister of the data subject.

[186] The justification of property rights entails several problems of general, specific, and particular justification: Why should there be any property rights at all? What kinds of property rights should there be? Who, in particular, should be entitled? (Lawrence C. Becker, The Moral Basis of Property Rights, id, at p. 187).

[187] Robert Bartlett, Developments in the Law: The Law of Cyberspace, Harvard Law Review, 1999, Vol. 112, pp. 1574-1704 (available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=3391&context=facpubs), at p. 1647, where the author argues that a property rule would be preferable to a liability rule for the protection of privacy as the (proposed by Bartlett) P3P (Platform for Privacy Preferences) regime, reducing privacy transaction costs, would result in the optimal level of privacy protection; it permits individuals to value privacy according to their personal preferences. See also Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, Berkeley Technology Law Journal, 1996, Vol. 11, No. 1, pp. 1-92 (available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1133&context=btlj), at pp. 4, 76, 78, where Mell supports that the resolution of the problem of regulating the "*myriad*" interests in the "persona" (i.e. a personal information file electronically stored, which, by virtue of at least one identifier relates the personal information to a specific person) should begin with reference to the law of property, as its concepts have long been used to balance competing interests in valuable resources. To Mell, the "persona" should be regarded as property, "*the ultimate ownership or fee simple of which resides in the individual*". This way, privacy would allow the person to regulate the extent to which third parties could obtain information concerning her and to monitor and correct the accuracy of her information. See also J.E.J. Prins, The Propertization of Personal Data and Identities, Electronic Journal of Comparative Law, Vol. 8.3, October 2004 (available at https://www.ejcl.org/83/art83-1.PDF), pp. 1-7, at p. 5, arguing that personal data, being almost by definition part of the public domain, are widely available, obtainable, and usable; this might not change, if property rights were introduced, as, in reality, they would still be widely available ("[…] *Even if personal data were to be protected by technologies such as P3P* […] *or other technical negotiating protocols, individuals would nevertheless be willing, required or forced to make their data available for use by third parties* […]").

[188] Chih-Liang Yeh, Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers, Telecommunications Policy, 2018, Vol. 42, Issue 4, pp. 282-292, available at https://doi.org/10.1016/j.telpol.2017.12.001.

invest heavily in their processing[193]. Some commentators, condemning the above practices, speak of "theft of our souls"[194].

But, since personal data are intangible and, thus, incapable of being subjected to rules that govern physical property[195], could intellectual property[196] laws apply?

A Moral Rights-Like Approach

In the European Union and several nations, authors enjoy their moral rights[197] in the works they create[198]. To some, having a moral right to the fruits of one's labor might also mean having a right to

---

[189] Lucie Guibault, Wrapping Information in Contract: How does it affect the Public Domain, in L. Guibault and P. B. Hugenholtz (eds), The Future of the Public Domain, id, pp. 87-104, at pp. 94, 104 (mentioning that the end-user's actions are often restricted under the terms of use set out by the provider and observing that there is a growing tendency to distribute information subject to the terms of online standard form contracts).

[190] Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at p. 230 (where it is argued that information, including personal data, is seen as a commodity that can be traded against a discount in the virtual supermarket or some other benefit, like access to a service).

[191] See Joaquín Almunia's speech (Nov. 26, 2012) "Competition and personal data protection" (mentioning that "[…] *Today, personal data are a type of asset for companies* […]"). Available at http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.

[192] See Eli Pariser, The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think, Penguin Group, 2011, at p. 16.

[193] Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at p. 230 ("[…] *Data marketers and other commercial organizations invest heavily in data processing techniques because it is worth the money and risk* […]").

[194] As Mann argues, a notion like violation of privacy is not as strong as a notion like "*Theft*". Steve Mann, Computer Architectures for Protection of Personal Informatic Property: Putting Pirates, Pigs, and Rapists in Perspective, id. Mann defines "humanistic property" (HP) as "[…] *the personal informatic property that is not the fruits of our intentional labour* […] *that which we generate simply through our natural existence doing other things* […] *HP includes, for example, our own physical likeness, knowledge of which door we passed through to enter our home, and records of how much milk we consumed or how many condoms we purchased over the past year* […]". To others, the dishonest use of an individual's identity by another person is more than fraud. Clare Sullivan, Digital Identity: An emergent legal concept (the role and legal nature of digital identity in commercial transactions), 2011, University of Adelaide Press, at p. 116 (see also at p. 121 mentioning that for the purposes of theft, property is regarded as belonging to the person who has control of it or who has a proprietary right in it).

[195] For a discussion see Kenneth C. Laudon, Markets and Privacy, id, at p. 93, where mechanisms, based on individual ownership of personal information and a "*National Information Market*", are proposed to ensure that individuals would receive fair compensation for the use of their data (see also at p. 92, asking "[…] *Why not let individuals own the information about themselves and decide how the information is used?* […]").

[196] Intellectual Property refers to intangible interests in commercially valuable products of the human intellect. See Garner Bryan, Black's Law Dictionary, 10th Edition, 2014, Thomson West. The interests are intangible, meaning that one does not possess intellectual property in the same way as one possesses tangible property, such as land or a chair. See Melamed Douglas, Picker Randal, Weiser Philip, Wood Diane, Antitrust Law and Trade Regulation, Cases and Materials, 7th Edition, 2018, Foundation Press, at p. 891.

possess and personally use what a person develops[199]. Moral right provisions assume a bond between the author and the work[200] and aim to protect the reputation of the author[201].

These rights, deriving from the conceptualization of creations reflecting the author's personality, include[202]: the right to integrity, to preserve the integrity of the author (and the integrity of the work) and to use the work as the author intended; the right to attribution or "paternity"; the right to disclose (to decide when a work should first be made available to others); and the right to withdrawal, allowing the author to retrieve a work from its current owner, provided the owner is compensated for the loss[203].

Moral rights strike a balance between the right to transform a work for profit or creativity and the right to the integrity of the work that will preserve its cultural or social[204] value[205]. As authors have observed, jurisdictions that recognize moral rights restrict creators in the extent to which they can transfer or

---

[197] See Article 6bis of the Berne Convention for the Protection of Literary and Artistic Works, mentioning "[…] *(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation. (2) The rights granted to the author in accordance with the preceding paragraph shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the country where protection is claimed. However, those countries whose legislation, at the moment of their ratification of or accession to this Act, does not provide for the protection after the death of the author of all the rights set out in the preceding paragraph may provide that some of these rights may, after his death, cease to be maintained. (3) The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed* […]".

[198] Margaret Ann Wilkinson, Natasha Gerolami, The author as agent of information policy: The relationship between economic and moral rights in copyright, in Government Information Quarterly, 2009, Vol. 26, pp. 321-332, at pp. 325-327, who briefly discuss the history of moral rights.

[199] Edwin C. Hettinger, Justifying Intellectual Property, in Philosophy & Public Affairs, Vol. 18, No. 1, Winter 1989), pp. 31-52, at p. 39.

[200] Raymond Sarraute, Current Theory on the Moral Right of Authors and Artists under French Law Source, The American Journal of Comparative Law, Vol. 16, No. 4 (Autumn, 1968), Oxford University Press, pp. 465-486, at p. 465, mentioning that moral right includes "[…] *non-property attributes of an intellectual and moral character which give legal expression to the intimate bond which exists between a literary or artistic work and its author's personality; it is intended to protect his personality as well as his work* […]".

[201] Margaret Ann Wilkinson, Natasha Gerolami, The author as agent of information policy, id, at p. 327 (with further references).

[202] Charles R. Beitz, The moral rights of creators of artistic and literary works, The Journal of Political Philosophy, Vol. 13, No. 3, 2005, pp. 330-358, at p. 332 (with further references to French case-law).

[203] For an analysis, see Paul Goldstein & Bernt Hugenholtz, International Copyright: Principles, Law, and Practice, 3rd Edition, Oxford University Press, 2013, at pp. 357-369.

[204] "Moral" should not be understood as the opposite of "immoral" or "amoral"; the term conveys an element of ethics or a societal interest. Susan Liemer, Understanding Artists' Moral Rights: A Primer, Boston University Public Interest Law Journal, 1998, Vol. 7, pp. 41-57, at p. 42. Available at https://ssrn.com/abstract=1132887.

[205] Margaret Ann Wilkinson, Natasha Gerolami, The author as agent of information policy, id, at p. 328.

waive them[206]. Furthermore, these rights are enforceable against any subsequent owner of the work and there is no requirement of privity[207], as there would be in case of contracts.

So, could such rights be granted for the protection of personal data?

As noted above, the right to the protection of personal data is an aspect of the right to privacy[208]. But the very notion of privacy is difficult to define. Simply put, privacy serves a range of interests, including personal autonomy, integrity and dignity, which, in turn, have a broader societal significance[209]. So, a *quasi* moral right, establishing a bond between the person and her data, would allow the individual to "possess and personally use" such information. The data subject would enjoy the right to integrity[210]; to preserve the integrity of herself and her data[211] and to use her information as she would intend. A right to attribution or "paternity" and a right to disclose would allow the individual to decide when her data should be made available to others, while the right to withdrawal would enable her to retrieve her personal information from the "current owner". Besides, the right to the protection of personal data is a fundamental human right and, as such, it cannot be waived or transferred[212].

---

[206] Charles R. Beitz, The moral rights of creators of artistic and literary works, id, at p. 332, mentioning that moral rights are perpetual and inalienable.

[207] Charles R. Beitz, The moral rights of creators of artistic and literary works, id, at p. 334.

[208] Maria Bottis, The protection of private life and the European Legislation with regard to Personal Data: Thoughts on the protection of private life in the USA, id.

[209] Lee A. Bygrave, Data Privacy Law, an International Perspective, Oxford University Press, 2014, pp. 1-266, at pp. 119-120; Alexandra Rengel, Privacy as an International Human Right and the Right to Obscurity in Cyberspace, Groningen Journal of International Law, Vol. 2, No. 2, 2014, Privacy in International Law, pp. 33-54.

[210] Integrity is an important principle of personal data processing. See Article 5(1)(f) of the GDPR ("[…] *Personal data shall be* […] *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures* […]").

[211] As some have argued, as regards the rationales of moral rights, a work can be understood as an expression of the author's "*innermost being*". John Henry Merryman, The refrigerator of Bernard Buffet (1976), in John Henry Merryman, Albert Elsen, Stephen Urice (eds), Law, Ethics and the Visual Arts, Fifth Edition, Kluwer Law International, 2007, The Netherlands, pp. 421-424, at p. 423. But see Amy M. Adler, Against Moral Rights, California Law Review, 2009, Vol. 97, Issue 1, pp. 263-300, at p. 265 (questioning "*does moral rights law make sense in an era in which "art", at least as we have known it for centuries, is over?*").

[212] European courts support that human rights reflect personal integrity and liberty; it is an established position of jurisprudence that the Convention for the Protection of Human Rights and Fundamental Freedoms does not protect a right to obtain remuneration for the waiver or sacrifice of a fundamental human right. See *Mellacher* case (E.C.H.R., *Mellacher v. Austria*, 1989, 12 E.H.R.R. 391); Nadezhda Purtova, Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation (October 25, 2009), European Journal of Legal Studies, Vol. 2, No. 3, 2010, pp. 193-208, at p. 203. In accordance with the above positions, privacy, as a human right inseparable from personhood, cannot be waived or transferred. Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at pp. 234-237. However, as noted above, there have been cases, in which the European Court of Human Rights has held that an individual may consent to waiving a fundamental right, albeit has to do so in an explicit manner. See *Deweer/Belgium*, ECHR, id; *De Wilde, Ooms, Versyp/Belgium*, ECHR, id.

So, the potential granting of such rights could address some aspects of the data protection problem and, in particular, the aspects of the lost control and the lack of secrecy[213]. But the greatest advantage of a moral rights-like approach is that these rights would be enforceable against any person beyond those with whom a data subject would have contracted. Indeed, they could be asserted against firms that process data and are often not in privity with the data subject, whose information is used. So, the aspect of otherness could also be addressed, as any individual, not being party to a contract, albeit being affected by the processing, would enjoy protection.

However, moral rights refer to a work, a product of the human mind that demands some effort or action, whereas personal data are created unconsciously and without any effort[214]; people produce data because they just live their lives. Besides, moral rights are not supposed to function as commodities and it is widely thought wrong to allow them to be exchanged[215]. So, this might disregard the current status of personal data, which do have value. And if data's value were not recognized, how could one address the aspect of its unequal distribution?

A Sui Generis Rights-Like Approach

Under Article 1(2) of the Directive 96/9/EC[216], database shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. In accordance with the above Directive 96/9/EC original and unoriginal databases are protected.

Databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation are protected as such by copyright[217]. In this case, protection does not extend to the content[218]. On the other hand, with regard to unoriginal databases, the maker of a database, which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents, has the right to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database[219]. So, on the basis of qualitative or quantitative investment unoriginal databases and their contents may be protected with a *sui generis* right[220] that expires fifteen years from

[213] For a discussion on moral rights' potential as regards control over data, see Henry Pearce, Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?, Information & Communications Technology Law, 2018, Vol. 27, No. 2, pp. 133-165, at pp. 153-159.

[214] Steve Mann, Computer Architectures for Protection of Personal Informatic Property: Putting Pirates, Pigs, and Rapists in Perspective, id.

[215] Charles R. Beitz, The moral rights of creators of artistic and literary works, id, at p. 335.

[216] See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, hereinafter referred to as Directive 96/9/EC.

[217] See Article 3(1) of the Directive 96/9/EC.

[218] See Article 3(2) of the Directive 96/9/EC.

[219] See Article 7(1) of the Directive 96/9/EC.

[220] The Directive 96/9/EC introduced a *sui generis* intellectual property right in databases in addition to "normal" copyright. Mireille van Eechoud, Along the Road to Uniformity - Diverse Readings of the Court of Justice Judgments on Copyright Work, JIPITEC, 2012, Vol. 3, Issue 1, pp. 60-80, at p. 61. Interestingly, this right protects the "*sweat of the brow*" of the database producer, meaning the skill, labor and financial means invested in the database. This test closely resembles the "*skill and labor*" test that was applied in several jurisdictions until the originality standard of the "*author's own intellectual creation*" was introduced. Bernt Hugenholtz, Something Completely Different: Europe's *Sui Generis*

the year following the date of completion[221]. But any substantial change to the contents of a database qualifies the database for its own term of protection[222]. So, protection extends to the content of a database, such as simple facts, data or elements that used to belong in the public domain[223]. And this *sui generis* protection may last for a fifteen-year-period, albeit, given the potential of renewal of this period after any substantial change[224] to the content, which is indeed constantly being updated, this protection is for 15 years or eternity, whichever is longer[225].

So, do personal data constitute the content of a database?

The answer may seem straightforward, but, to better understand the extent to which personal data may be collected in private databases, Cloud Computing technologies should be examined.

Today, users can store information in the "clouds"[226] and firms can collect data, referring not only to consumers themselves but also to third parties. Namely, via services, like Google Drive or Dropbox, an individual may upload her data, e.g. a personal image, or third parties' information, e.g. an image downloaded from the Web. Besides, such activities may be undertaken to ensure integrity and successful management of people's data; one may use Cloud Computing services to avoid potential deletion of her files, due to e.g. malware/virus attacks, wastage of the personal computer's storage space or use of external devices. So, a lawyer can use Cloud to upload and further process her documents (e.g. applications), while physicians may store files that could include patients' sensitive data.

This way, individuals entrust their information to a provider; a lawyer will store her files in the Cloud and will, then, modify an existing statement or application; hence, this document will be produced

---

Database Right, in Susy Frankel & Daniel Gervais (eds), The Internet and Emerging Importance of New Forms of Intellectual Property, Information Law Series, Wolters Kluwer, 2016, pp. 205-222, at p. 212. Hugenholtz argues that the database right may be qualified as a right of Intellectual Property that either falls within the very loosely organized rubric of neighboring rights or as a right of Intellectual Property of its own kind, i.e., truly *sui generis*. But, whatever its classification, this right most certainly is not a copyright. Bernt Hugenholtz, id, at p. 218. Indeed, some European member states, including Germany, classify this right as a neighboring right, while others, like France or the Netherlands, treat it as a right of its own category. NautaDutilh, The implementation and application of Directive 96/9/EC on the legal protection of databases, Study – Contract ETD/2001/B5-3001/E/72, available at http://ec.europa.eu/internal_market/copyright/docs/studies/etd2001b53001e72_en.pdf.

[221] See Article 10(1) of the Directive 96/9/EC.

[222] See Article 10(3) of the Directive 96/9/EC.

[223] James Boyle, Foreword: The Opposite of Property?, id, at p. 25; Giancarlo Frosio, Communia and the European Public Domain Project: A Politics of the Public Domain, in Melanie Dulong de Rosnay & Juan Carlos De Martin (eds), The Digital Public Domain: Foundations for an Open Culture, pp. 3-45, at p. 25 (available at https://www.openbookpublishers.com/reader/93/#page/30/mode/2up); Mark Davison, Database Protection: The Commodification of Information, id.

[224] Under Recital 55 of the Directive 96/9/EC even a mere '*substantial verification of the contents of the database*' would suffice to trigger a new term of protection.

[225] Mark Davison, Database Protection: The Commodification of Information, id, at pp. 169, 187.

[226] While Big Data aims to transform decision-making, Cloud Computing aims to change the architecture. Daniel J. Abadi, Data Management in the Cloud: Limitations and Opportunities, Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, March 2009, Vol. 32, No. 1, pp. 3-12, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.717.4940&rep=rep1&type=pdf#page=5.

thanks to technologies that the provider offers and controls[227]. And, since information is a major source of income, it has to be kept in a secure place, i.e. the private data center (so-called "server center" or "storage facilities")[228]. So, Cloud Computing technologies refer both to applications provided as services and hardware or software located in these datacenters[229].

But providers may offer a wide variety of services. For instance, Google provides (to name but a few) data-storage services (Google Drive), e-mail services (Gmail), or word-processing services (Google Docs)[230]. Thus, it is in a firm's datacenter where a huge volume of data is stored; this may include any information that anyone may upload while using Cloud Computing services. As some have put it, such technologies have turned our work, finances, health and relationships into invisible data, centralized in out-of-the-way datacenters[231]. And, as data have independent value, are collected *en masse*, and may cover people's full personal or professional life, firms have found their way to safeguard their financial interests by processing information that anybody produces just by living her life[232].

So, personal data do constitute the content of a database. But could *sui generis* rights be granted?

The objective of the Directive 96/9/EC is to afford an appropriate and uniform level of protection of databases as a means to secure the remuneration of the maker of the database. This is different from the aim of personal data protection legislation. Besides, the legislator has made clear that the provisions of the Directive 96/9/EC are without prejudice to data protection legislation[233].

But a database is broadly defined as a collection of works, data or "*other materials*" and its content is generally described as "information" in the widest sense of that term[234]. Besides, courts have given an

[227] Chris Reed, Information "Ownership" in the Cloud, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 45/2010, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

[228] Evgeny Morozov, The Net Delusion, id, at p. 286.

[229] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report No. UCB/EECS-2009-28 (10 February 2009), pp. 1-23, at pp. 1-2. Available at https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[230] Examples of Cloud Computing technologies are Gmail or Google Docs (Software as a Service, SaaS), Microsoft Windows Azure or Google App Engine (Platform as a Service, PaaS), Amazon Elastic Compute Cloud (EC2) or IBM Computing on Demand (Infrastructure as a Service, IaaS). Christopher Yoo, Cloud Computing: Architectural and Policy Implications, Review of Industrial Organization, 2011, Vol 38, No. 4, pp. 405-421, at pp. 407-409; David Lametti, The Cloud: Boundless Digital Potential or Enclosure 3.0?, Virginia Journal of Law & Technology, 2012, Vol. 17, No. 3, pp. 190-243, at pp. 208-210.

[231] Gary Cook & Jodie Van Horne, How dirty is your Data? A look at the energy choices that power cloud computing, 2011, Greenpeace, at p. 4 (available at https://www.greenpeace.org/international/Global/international/publications/climate/2011/Cool%20IT/dirty-data-report-greenpeace.pdf).

[232] Julia Powles & Hal Hodson, Google DeepMind and healthcare in an age of algorithms, id, at p. 362 (mentioning that "[…] *It is a great stroke of luck that business has found a way to monetize a commodity that we all produce just by living our lives* […]").

[233] See Recital (48) of the Directive 96/9/EC.

[234] Bernt Hugenholtz, Something Completely Different: Europe's *Sui Generis* Database Right, id, at p. 211; Commission on the European Communities, Proposal for a Council Directive on the legal protection of databases, COM(92) 24 final, No C156/4, Official Journal of the European Communities (23.6.92), Explanatory Memorandum, paragraph 19.

expansive reading to include even online cloud services in health care[235], which qualify as databases. So, the potential granting of *sui generis* rights in case of personal data could be examined from, at least, a theoretical point of view.

As firms invest heavily in data processing, one could fairly argue that the criterion of qualitative or quantitative investment is met. Besides, the test of "substantial investment" is not hard to meet; any investment in a database that, viewed objectively, is not wholly insignificant and easy to be made by anyone would be sufficient[236]. However, procedures of collection, storage, and processing are opaque and one cannot know whether such data are arranged in a systematic or methodical way. Besides, even if personal data were arranged in such ways, they are not individually accessible by electronic or other means, since firms own their secret repositories of information. Although firms may provide access or exchange data with third parties, rather than individuals, albeit, one cannot speak of collections of data that are individually accessible.

Moreover, the Directive 96/9/EC protects the right of a database maker[237] to secure remuneration[238]. But if such rights were granted to protect personal data, the rightsholders should be the data subjects. Besides, one would demand the protection of each item of personal information (e.g. name, e-mail address, and so forth), instead of data's protection as the whole or a substantial part of the content of the database[239].

Things could get more complex if recent case law were taken into consideration.

In case *Ryanair Ltd v. PR Aviation BV*[240], PR Aviation operated a website on which consumers could compare prices and book flights. Data were obtained, amongst others, from a dataset linked to the Ryanair website that was also accessible to consumers[241]. Under Ryanair's terms and conditions, Ryanair.com was the only website authorized to sell Ryanair flights, while visitors were not permitted to use the website other than for private and non-commercial purposes[242].

The court found that Ryanair's database corresponds to the definition set out in Directive 96/9/EC[243]. But this does not justify the conclusion that it falls within the scope of the provisions governing copyright and/or the *sui generis* right, since the database fails to satisfy either the condition of

[235] The European Commission, Evaluation of Directive 96/9/EC on the legal protection of databases, (Brussels, 25.4.2018), SWD (2018) 146 final {SWD(2018) 147 final}, at p. 26 (citing UK national case *Technomed Ltd v Bluecrest Health* [2017] EWHC 2142).

[236] Bernt Hugenholtz, Data Property in The System of Intellectual Property Law: Welcome Guest or Misfit? in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds), Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden, Nomos 2017, pp. 75-99, at p. 86 (citing *Bundesgerichtshof*, 2010, Case 1 ZR 196/08, German Federal Supreme Court).

[237] See Article 7(1) of the Directive 96/9/EC.

[238] See Recital (48) of the Directive 96/9/EC.

[239] For a discussion on property rights in (compiled) data see, in general, Charles C. Huse, Database Protection in Theory and in Practice: Three recent cases, Berkeley Technology Law Journal, Annual Review 2005, Vol. 20, Issue 1, pp. 23-45, at pp. 44-45.

[240] See Judgment of The Court (Second Chamber), 15 January 2015, in Case C-30/14, *Ryanair Ltd v PR Aviation BV.* ECLI:EU:C:2015:10.

[241] *Ryanair Ltd v PR Aviation BV*, id, paragraph 15.

[242] *Ryanair Ltd v PR Aviation BV*, id, paragraph 16.

[243] See Article 1(2) of the Directive 96/9.

application for protection by copyright or the condition of application for the protection by the *sui generis* right[244]; the database was not original, while the criterion of qualitative or quantitative investment could not be met.

In particular, as the court ruled, if the author of a database protected by the Directive 96/9/EC authorizes the use, she has the option to regulate it by an agreement concluded with a lawful user. This agreement may set out the purposes and the way of using the database[245]. However, as regards a database to which the Directive 96/9/EC is not applicable, the author is not eligible for the system of legal protection set out by the Directive, so that she may claim protection only on the basis of the applicable national law[246]. Thus, the Directive 96/9/EC is not applicable to a database that is not protected either by copyright or by the *sui generis* right and it does not preclude the author from laying down contractual limitations on its use by third parties, without prejudice to the applicable national law[247].

In other words, by doing nothing, one can earn more. Namely, if one creates a database that is unoriginal and does not meet the investment criterion, she will be bound by the contract, i.e. the terms of service that she, herself, will prepare and which the user may never read. So, instead of devoting time, labor, and resources to achieve originality or investment, it is now preferable that the maker does nothing at all; the criteria will not be met, the Directive will not apply, and the database maker will enjoy the benefits that she will draft.

In fact, to the European Commission, the CJEU decision leads to the paradox that a database that is not protected by copyright or *sui generis* right may receive a stronger protection through contracts[248]. This could also mean that a database that is "*no more*" protected by copyright (meaning a public domain database) may receive the above protection through contracts[249]; or that "*any*" database that is "*simply not*" protected (by copyright or *sui generis* right, meaning or including "personal data databases") may enjoy this stronger protection.

Such uncertainties would most probably harm people's privacy.

In any case, failure to apply Intellectual Property rules (if *sui generis* rules are considered as such)[250] may be obvious for one more reason. Laws that govern Intellectual Property aim to offer incentives to create works and promote arts and science[251]. If such rights were granted for personal data, how fair

---

[244] *Ryanair Ltd v PR Aviation BV*, id, paragraph 35.

[245] *Ryanair Ltd v PR Aviation BV*, id, paragraph 43.

[246] *Ryanair Ltd v PR Aviation BV*, id, paragraph 44.

[247] *Ryanair Ltd v PR Aviation BV*, id, paragraph 45.

[248] The European Commission, Evaluation of Directive 96/9/EC on the legal protection of databases, id, at p. 32.

[249] The European Commission, Evaluation of Directive 96/9/EC on the legal protection of databases, id, at p. 32.

[250] As some authors have aptly observed "[…] *we create creatures like sui generis rights when we just don't know and can't validly guess what other, already existing right, is suitable or best for our case. When this unfortunate situation occurs in the context of medicine, we call a disease 'idiopathic' – meaning that we don't know what caused it or what it exactly is* […]". Maria Bottis, Law and information: a "love-hate" relationship, id, at p. 144.

[251] Mark A. Lemley, Private Property, Stanford Law Review, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May, 2000), pp. 1545-1557, at p. 1550.

would offering incentives to produce new data[252] be? This could lead to a dynamic competition among firms, as to which would collect and manage more and of better quality personal data; not just a dynamic competition, but also a race to the bottom, since the purpose of the hypothetical protection would be the promotion of processing practices in favor of the database makers' interests.

So, it seems that the right to the protection of personal data should not be treated as an Intellectual Property right. Besides, the former, contrary to the latter[253], is not an absolute right[254]. But before setting aside this hypothesis, let us examine another "secret" right that Intellectual Property rights (used to) include.

A Trade Secrecy-Like Approach

Under Article 1(1)(g) of the Commission Regulation (EC) No 772/2004 of 27 April 2004 on the application of Article 81(3) of the Treaty to categories of technology transfer agreements, intellectual property rights include industrial property rights, know-how, copyright and neighbouring rights. The above Regulation was replaced by the Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, under which intellectual property rights do not include know-how[255]. Besides, to the European Commission[256], trade secrets are not a form of (exclusive) intellectual property right.

However, some authors speak of a "*hidden*" Intellectual Property right[257], which compared with other types of Intellectual Property has several distinguishing features: it does not require registration; the subject matter is extremely broad as it encompasses any type of undisclosed information able to provide a competitive advantage to its owner; and the law does not provide an exclusive right to the holder of the secret[258].

---

[252] Viktor Mayer-Shönberger, Beyond Privacy Beyond Rights – Toward a "System" Theory of Information Governance, 98 California Law Review, 2010, Vol. 98, No. 6, pp. 1853-1886, at p. 1861; Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, id, at p. 250.

[253] As regards copyright, with the creation of their work authors obtain the intellectual property rights; these rights include, as exclusive and absolute rights, the right to exploit the work (economic right) and the right to protect their personal connection with the work (moral right). See EUIPO, FAQs on Copyright (available at https://euipo.europa.eu/ohimportal/en/web/observatory/faqs-on-copyright-el); Chandra Nath Saha and Sanjib Bhattacharya, Intellectual property rights: An overview and implications in pharmaceutical industry, Journal of Advanced Pharmaceutical Technology & Research, 2011 Apr-Jun, Vol. 2, Issue 2, pp. 88-93, at p. 88, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3217699/.

[254] See Recital (4) of the GDPR.

[255] See Article 1(1)(h) of the Commission Regulation (EU) No 316/2014; "[…] *'intellectual property rights' includes industrial property rights, in particular patents and trademarks, copyright and neighbouring rights* […]".

[256] See European Commission, Growth, Internal Market, Industry, Entrepreneurship and SMEs, Trade Secrets, available at http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en.

[257] Prajwal Nirwan, Trade secrets: the hidden IP right, WIPO Magazine, 6/2017, available at http://www.wipo.int/wipo_magazine/en/2017/06/article_0006.html.

[258] Luigi Alberto Franzoni & Arun Kumar Kaushik, The optimal scope of trade secrets law, International Review of Law and Economics, Volume 45, March 2016, pp. 45-53, at p. 46 (available at https://www.sciencedirect.com/science/article/abs/pii/S0144818815000708). See also James Pooley,

Regardless of whether or not trade secrets[259] constitute Intellectual Property rights, if personal data were treated as trade secrets, it seems that the individuals would better control their private information[260].

And could personal data be regarded as trade secrets[261]?

Personal data, which a firm may collect, are not generally known among or readily accessible to other firms that also collect data and are within the circles that normally deal with this kind of information[262]. Moreover, personal data have commercial value, deriving from the very fact that they are secret, and the person, lawfully in control of such data, i.e. the collector, takes or should take reasonable steps to keep data secret[263].

Trade Secrets: the other IP right, WIPO Magazine, 3/2013, who speaks of a "*kind*" of Intellectual Property right (available at http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html).

[259] Trade secrets (or know-how), differing from industrial property rights, copyright and neighbouring rights, have several advantages: they do not require disclosure, instead they require secrecy (whereas a condition for granting patents and copyrights is public disclosure of the invention or work); they are protected as long as they are kept secret (whereas most patents or copyright lapse after some period of time); they involve less cost than e.g. acquiring and defending other intellectual property rights. Edwin C. Hettinger, Justifying Intellectual Property, id, at p. 33. See also Article 1(1)(i) of the Commission Regulation (EU) No 316/2014 ("[…] *'know-how' means a package of practical information, resulting from experience and testing, which is: (i) secret, that is to say, not generally known or easily accessible, (ii) substantial, that is to say, significant and useful for the production of the contract products, and (iii) identified, that is to say, described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfils the criteria of secrecy and substantiality* […]").

[260] This could be achieved without limiting the free movement of such data. Gianclaudio Malgieri, Quasi-Property in Consumer Information: Trade Secrets and Consumer Rights in the Age of Big Personal Data, in Maria Bottis & Eugenia Alexandropoulou (eds), Proceedings of the 7th International Conference on Information Law and Ethics, ICIL 2016, Broadening the Horizons of Information Law and Ethics, A Time for Inclusion, pp. 376-400, Greece, Thessaloniki, University of Macedonia Press (available at https://icil.gr/2016/icil/proceedings/). Besides, rules that govern trade secret ensure control enabling the secret holder to keep her information well-hidden and benefit from its exploitation. See, in general, Luigi Alberto Franzoni & Arun Kumar Kaushik, The optimal scope of trade secrets law, International Review of Law and Economics, Volume 45, March 2016, pp. 45-53.

[261] Under Article 2(1)(a-c) of the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (hereinafter referred to as "Directive (EU) 2016/943"), "trade secret" means information which: is secret, in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; has commercial value, because it is secret; and has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

[262] Namely, one's passport number, collected by a firm that offers accommodation services, is not generally known among other companies that process such data, nor is it readily accessible to such companies. It may be true that, under a firm's terms of service, the provider may share one's data with other parties, but for the sake of simplicity it will be considered that such data are secret, within the meaning of Article 2(1)(a) of the Directive (EU) 2016/943.

[263] At least this is what providers claim. For instance, Amazon claims that they use Secure Sockets Layer (SSL) software to encrypt information users input ("[…] *We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input* […]". Available at https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_3DF674DAB5B7439FB2A9B4465BC3E0AC.

The potential treatment of personal data as *quasi* trade secrets would guarantee an adequate protection[264]: as any item of information can be protected by trade secrecy rules[265], the protection of each personal datum would be achieved; individuals, as licensors, would provide data to firms for a particular purpose; and it would be prohibited to use such data for other purposes without the licensor's permission[266], or to further transfer license rights without the initial licensor's consent[267]. Besides,

[264] One could further argue that personal data ought to fulfill the trade secret's definition. In fact, personal information ought to be secret, in the sense that it should not be generally known or readily accessible to persons within the circles that normally deal with the kind of information in question. Since personal data may be subject to exploitation, they should have commercial value due to the fact that they need to be secret. Finally, a firm, lawfully in control of personal data, should take reasonable steps to keep data secret. Besides, right to the protection of personal data is not an absolute right (Recital (4) of the GDPR). Similarly, trade secret rights are not absolute, nor are they exclusive. Mark A. Lemley, The Surprising Virtues of Treating Trade Secrets as IP Rights, in Rochelle C. Dreyfuss & Katherine J. Strandburg (eds), The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research, Edward Elgar Publishing, 2011, pp. 109-139, at p. 122 ("[…] *The right of exclusion in trade secret law is not absolute* […]"); Recital (16) of the Directive (EU) 2016/943 ("[…] *In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets* […]").

[265] Trade secret protection extends to the very data, like information on customers. See Recital (2) of the Directive (EU) 2016/943, where it is mentioned that confidentiality is used by businesses as a competitiveness and research innovation management tool, and "*in relation to a diverse range of information that extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans, and market research and strategies*".

[266] Under Article 4(2)(a, b) of the Directive (EU) 2016/943, the acquisition of a trade secret without the consent of the trade secret holder should be considered unlawful, whenever carried out by: unauthorized access to, appropriation of, or copying of any -data such as- documents, objects, or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced; any other conduct that under the circumstances is considered contrary to honest commercial practices. Besides, the use or disclosure of a trade secret should be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person, who has acquired the trade secret unlawfully, or has been in breach of a confidentiality agreement or any other duty not to disclose the trade secret (or duty to limit the use of the trade secret). See Article 4(3)(a-c) of the Directive (EU) 2016/943. The acquisition, use, or disclosure of a trade secret should also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been unlawfully obtained. See Article 4(4) of Directive (EU) 2016/943.

[267] When the licensor provides data (as a trade secret) to another for a particular purpose, this information cannot be used for other purposes without obtaining the licensor's permission; the license rights may be further transferred by the licensee, only if such right to sublicense has been agreed, meaning only if the initial licensor has given her consent. Pamela Samuelson, Privacy As Intellectual Property?, Stanford Law Review, 1999, Vol. 52, pp. 1125-1173, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3137&context=facpubs, at pp. 1155-1156; Terry B. Mcdaniel, Shop Rights, Rights in Copyrights, Supersession of Prior Agreements, Modification of Agreement, Right of Assignment and Other Contracts, AIPLA Q.J., 1986, Vol. 14, pp. 35-48, at pp. 45-47 (available at https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/aiplaqj14&id=48). For sub-licensing and sub-processing of data, see W. Kuan Hon, Christopher Millard, Ian Walden, Who is responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Pt. 2, in International Data Privacy Law, Volume 2, Issue 1, 1 February 2012, pp. 3-18 (available at https://academic.oup.com/idpl/article/2/1/3/730143).

confidentiality[268] and trade secret rights should be used as business competitiveness and research innovation management tool[269]. Hence, via a trade secrecy-like approach, a dynamic competition would, perhaps, emerge. And, maybe, stronger guarantees would be provided, as regards transparent processing and high-quality services to the end user, i.e. the initial licensor. Firms would probably be unable to transfer data to third parties without the subject's permission, while they might also endorse new technologies to transparently and rationally process personal data for specific purposes, which would be determined by the initial licensor[270].

So, the above trade secrets-like approach could probably address some aspects of the data protection problem and, in particular, the absence of control, the lack of secrecy, and (indirectly, as general rules would apply) the unequal distribution of data's value. However, such rights would not be enforceable against any person beyond those with whom an individual would have contracted; they could not be asserted against firms that process data but are often not in privity with the data subject. Hence, the trade secrecy-like approach would most probably not address the aspect of otherness; an individual, who would not be party to a contract but who would be affected or influenced by the processing, would not enjoy protection[271].

Besides, trade secrecy refers to an "idea", and it might not be reasonable to treat people's names and addresses as "the Coca-Cola's formula"[272]. The latter could be considered as a "pure product" and this might run counter to integrity, dignity, and other values, to which privacy relates[273].

Even though authors[274] suggested treating personal information as a property right more than fifty years ago[275], such rights could raise significant policy or free speech issues[276]. Indeed, it would be abnormal to imagine persons being private owners of facts, whose use they would be entitled to restrict. Besides, the *raison d' être* of property is alienability; the purpose of property laws is to prescribe the conditions of transfer[277].

---

[268] Confidentiality is a general principle relating to personal data processing. See Article 5(1)(f), Recitals (39), (49) and (83) of the GDPR.

[269] See Recital (2) of the Directive (EU) 2016/943.

[270] Pamela Samuelson, Privacy As Intellectual Property?, id.

[271] Trade secrets, like other "non-property" regimes, do not create rights *erga omnes*, so "[…] *valuable data are at risk of being misappropriated* […]". Bernt Hugenholtz, Data Property in The System of Intellectual Property Law: Welcome Guest or Misfit?, id, at pp. 79-80.

[272] For some information on the Coca-Cola's formula, see Christopher Scott Harrison, The Politics of the International Pricing of Prescription Drugs, 2004, Praeger Publishers, Westport, Connecticut, London, at pp. 14-16.

[273] Lee A. Bygrave, Data Privacy Law, an International Perspective, id; Alexandra Rengel, Privacy as an International Human Right and the Right to Obscurity in Cyberspace, id.

[274] Alan F. Westin, Privacy and Freedom, 1967, New York, Atheneum.

[275] And, interestingly, authors still argue for this approach. Václav Janeček, Ownership of personal data in the Internet of Things, 2018, Computer Law & Security Review (forthcoming – available at https://www.sciencedirect.com/science/article/pii/S0267364918300487), pp. 1-14.

[276] Wendy J. Gordon, On Owning Information: Intellectual Property and the Restitutionary Impulse, Virginia Law Review, 1992, Vol. 78, pp. 149-281, at pp. 267-281 (available at https://open.bu.edu/bitstream/handle/2144/22968/78VaLRev149_web.pdf?sequence=1); J.H. Reichman and Pamela Samuelson, Intellectual Property Rights in Data? Vanderbilt Law Review, 1997, Vol. 50, pp. 51-166, at p. 64-72 (available at https://www.law.berkeley.edu/php-programs/faculty/facultyPubsPDF.php?facID=346&pubID=66).

[277] Jessica Litman, Information Privacy/Information Property, id, at pp. 1295, 1301 (mentioning that the market in personal data is the problem and that market solutions based on a property rights model will not cure it; they will only legitimize it).

So, could there be another approach[278] outside the property sphere?

[278] It should be mentioned that some authors have proposed a tort model, where the personal data processor would be liable for the failure to use Fair Information Practices. The tort would apply to any entity that would process information linked with an individual and it would protect the individual's interests in choice (about who may receive the data) and control (over the data revealed and how the recipient may use it). In this concept, damages would also be awarded based on injuries to the individual's choice and control. Sarah Ludington, Reining in the Data Traders: A Tort for the Misuse of Personal Information, Maryland Law Review, 2006, Vol. 66, pp. 140-193, at pp. 173-174, 189. Ludington argues that the most positive effect of such tort would be the creation of an incentive for data traders to invest in better data security technologies. They would take seriously their obligation to use Fair Information Practices and implement better systems of obtaining consent. But, to others, such an approach would not be effective, as tort law protects personal data from disclosure only when it conveys embarrassing personal information. Jessica Litman, Information Privacy/Information Property, id, at p. 1291 (with further references).

Chapter V. Personal Data Fiduciaries

Many years ago, a man named John Moore underwent treatment for hairy-cell leukemia. The physicians removed Moore's spleen for therapeutic reasons, but they detected some unique characteristics in the tissue of the spleen that could be further researched and developed. So, they used the blood samples both for Moore's treatment and unrelated research. When Dr. David Golde patented the cell line and entered into agreements for its commercial development, Moore sued for conversion of his cells; he argued that the exploitation invaded his privacy interests in the parts of his body. The court rejected the claim to ownership, albeit, it upheld the complaint on the ground that Dr. Golde had breached his fiduciary duty, as he had failed to disclose his intention to further use the cells and to obtain Moore's informed[279] consent[280].

While any law may illustrate societies' values and norms, fiduciary[281] law reflects them with great clarity; it regulates relationships based on trust[282]. And trust[283], including honesty, truth telling, and

[279] In medical fields, informed consent refers to an ethical and legal doctrine; all interventions should only be performed after a participant has been informed about the purpose, nature, consequences, and risks, and has freely consented. Salman Yousuf Guraya, N.J.M. London, Shaista Salman Guraya, Ethics in medical research, Journal of Microscopy and Ultrastructure, 2014, Vol. 2, pp. 121-126, at p. 123 (mentioning also that the primary focus concerning consent should be on informing and protecting research subjects, through disclosure and discussion of relevant information, meaningful efforts to promote understanding, and by ensuring that decisions to participate are always made voluntarily; "[…] *Informed consent is the ethical cornerstone* […]").

[280] *Moore v. Regents of University of California* (No. S006987, Supreme Court of California, Jul 9, 1990, available at https://law.justia.com/cases/california/supreme-court/3d/51/120.html); Maureen S. Dorney, *Moore v. the Regents of the University of California*: Balancing the Need for Biotechnology Innovation against the Right of Informed Consent, Berkeley Technology Law Journal, 1990, Vol. 5, Issue 2, pp. 333-369.

[281] The term "fiduciary" comes from the Latin verb "fidere" that means to "trust". Fiduciary duty is a legal term that refers to the type of duty that a person or organization, who manages someone else's power, wealth or property, has in certain circumstances in relation to the owner or beneficiary of that power, wealth or property. So, fiduciary duties are legal obligations that exist in certain situations between one party (the beneficiary) that owns or has the rights to assets or power that another party (the fiduciary or trustee) manages. The European Commission, Resource Efficiency and Fiduciary Duties of Investors, Final Report, ENV.F.1/ETU/2014/0002, DG Environment, at p. 22. Available at http://ec.europa.eu/environment/enveco/resource_efficiency/pdf/FiduciaryDuties.pdf.

[282] See, in general, Tamar Frankel, Fiduciary Law, California Law Review, 1983, Vol. 71, No. 3, pp. 795-836, available at https://scholarship.law.berkeley.edu/californialawreview/vol71/iss3/1/.

[283] Trust may be understood as the willingness to accept vulnerability to the actions of others. It is an essential element of any activity, in which people are involved (e.g. friendship, commerce etc). Ethan J. Leib, Friends as Fiduciaries, Washington University Law Review, Vol. 86 (2008-2009), pp. 665-732, at p. 693 (mentioning that a high degree of trust necessarily leads to a substantial degree of vulnerability); Annette C. Baier, Trust and Antitrust, Moral Prejudices: Essays on Ethics, 1994, Harvard University Press, at p. 133 (mentioning that "[…] *Trust is accepted vulnerability to another's power to harm one, a power inseparable from the power to look after some aspect of one's good* […]"). As others have put it, trust is "*a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*". Denise M. Rousseau, Sim B. Sitkin, Ronald S. Burt, Coun Camerer, Introduction to special topic forum not so different after all: A cross-discipline view of trust, Academy of Management Review, 1998, Vol. 23, No. 3, pp. 393-404, at pp. 394-395. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.8322&rep=rep1&type=pdf. See also

keeping promises[284], highlights everything we have accomplished as human species[285]. Trust could be regarded as the key element of healthy relationships and societies[286] enabling an individual to be willing to make herself vulnerable to another party, to rely on another, despite potential risks that the latter will act in a way that can harm the former[287]. So, in the context of privacy, trust would mean the willingness to become vulnerable to a person or entity by sharing personal data. The individual, disclosing the data, would be the entrustor; the act of disclosing/sharing would be the entrusting; and the recipient/processor of the data would be the entrustee. And it would be fair to argue that today we are all entrustors, entrusting firms when disclosing information to a search engine or any digital firm. And given the nature and volume of personal data revealed (e.g. items of sensitive information included in an e-mail), perhaps, people trust data processors even more than they trust their lawyers, whom the law treats as fiduciaries. So, one becomes vulnerable, when she faces the risk of misuse or unauthorized disclosure of her data. Namely, vulnerability may refer to the potential risk of an employee being fired, or the risk of selling data to third parties.

If the concept of trust were introduced in privacy regime and laws, it could further enable honesty and loyalty[288]. In particular, fiduciaries provide services that are socially important and it is in the interest of society that people use them[289]. In fact, individuals need experts to rely on and it would make no

---

Ethan J. Leib, Friendship & The Law, UCLA Law Review, Vol. 54, 2007, pp. 631-707, at p. 643 with further references ("[…] *Trust is a belief that another will fulfill his or her obligations and pull his or her weight in a relationship* […]"); Merriam – Webster dictionary (defining trust as "*assured reliance on the character, ability, strength, or truth of someone or something* […] *one in which confidence is placed* […] *a charge or duty imposed in faith or confidence or as a condition of some relationship* […] *something committed or entrusted to one to be used or cared for in the interest of another* […]"), available at https://www.merriam-webster.com/.

[284] James Post, Governance, Accountability, and Trust: A comment on the work of Tamar Frankel, Boston University Law Review, 2011, Vol. 91, pp. 1165-1173, at pp. 1165-1166 (citing Frankel, whose "[…] *definition of trust is appealingly straightforward: Trust is 'reasonably believing that others tell the truth and will keep their promises'* […]"). Available at http://www.bu.edu/law/journals-archive/bulr/documents/post.pdf.

[285] Bruce Schneier, Data and Goliath, id, at p. 212, mentioning that trust is personal, relative, situational, and fluid.

[286] See, in general, Francis Fukuyama, Trust: The Social Virtues and The Creation of Prosperity, Free Press Paperbacks, 1996, USA.

[287] In commercial relationships, trust begins with the promise that leads to a contract. Eli Bukspan, Trust and the Triangle Expectation Model in Twenty-First Century Contract Law, 11 DePaul Bus. & Com. L.J., 2013, pp. 379-415, at pp. 382-383. Available at: http://via.library.depaul.edu/bclj/vol11/iss3/4. In fields of personal relationships, the quality of a friendship depends on the extent of trust between people. Irwin Altman, Reciprocity of Interpersonal Exchange, Journal of the theory of social behavior, Vol. 3, Issue 2, October 1973, pp. 249-261. Available at https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-5914.1973.tb00325.x.

[288] One of the most important fiduciary duties is the duty of loyalty, meaning that fiduciaries should act in good faith in the interests of their beneficiaries and impartially balance the conflicting interests of different beneficiaries. They should avoid conflicts of interest and should not act for the benefit of themselves or a third party. Another important duty is the duty to act prudently, which means that fiduciaries should act with due care, skill and diligence. The European Commission, Resource Efficiency and Fiduciary Duties of Investors, id, at p. 7. In either case, the objective is to encourage the fiduciary to take the beneficiary's interests properly into account in making decisions and to facilitate detection of her failure to do so. Elizabeth S. Scott and Robert E. Scott, Parents as Fiduciaries, Virginia Law Review, Vol. 81, No. 8, Symposium: New Directions in Family Law (Nov. 1995), pp. 2401-2476, at pp. 2420-2421.

[289] Jack M. Balkin, Information Fiduciaries and the First Amendment, UC Davis Law Review, 2016, Vol. 49, No. 4, pp. 1183-1234. Available at https://ssrn.com/abstract=2675270.

sense for everyone to become, e.g., a lawyer to handle her own case. In this context, fiduciaries cannot perform unless they are entrusted with power; a physician[290] must have full control over the patient's body to operate on her. And this entrustment has a single goal, i.e. to facilitate services to the entrustors[291]. Thus, the risk that fiduciaries may use the entrusted power for purposes other than in the service of the entrustors involves competition among fiduciaries, who have to convince beneficiaries they use the relevant power for the entrustors' benefit[292].

But there are many topics to which the label "fiduciary" can be applied[293] and the duties of fiduciaries may vary. However, the general and most important duty of loyalty, the duty to act for the exclusive benefit of the beneficiary[294], could be introduced for the protection of personal data. Indeed, an individual entrusts firms her data, over which they have control. They are the experts, who are (capable of) providing socially useful services and it would make no sense for us to become data scientists, process our data and "make them speak" or develop algorithms that would make genius decisions concerning our well-being. One could further argue that, under this approach, fiduciaries could have

[290] In some jurisdictions, physicians have been members of the "fiduciary group" since, at least, 1965. See *Hammonds v. Aetna Casualty & Surety Company*, 243 F. Supp. 793 (N.D. Ohio 1965), at 802, mentioning that "[…] *all reported cases dealing with this point hold that the relationship of physician and patient is a fiduciary one* […]".

[291] To some, this is the "*fiduciary duty*". L. S. Sealy, Fiduciary Relationships, The Cambridge Law Journal, Vol. 20, Issue 1 (April 1962), pp. 69-81; Robert Cooter & Bradley J. Freedman, The fiduciary relationship: Its economic character and legal consequences, New York University Law Review, 1991, Vol. 66, pp. 1045-1075. Others regard the duty of loyalty as a response to the impossibility of writing contracts completely specifying the parties' obligations. Frank H. Easterbrook, Daniel R. Fischel, Contract and fiduciary duty, The Journal of Law and Economics, The University of Chicago Law School, Vol. XXXVI, April 1993, pp. 425-446, at p. 426.

[292] Tamar Frankel, Fiduciary law in the twenty-first century, Boston University Law Review, 2011, Vol. 91, pp. 1289-1299, at p. 1294 (see also at p. 1298, observing that fiduciary law reflects the degree of temptation to which fiduciaries are exposed: the larger the entrusted amounts, the greater the temptation). Available at https://www.bu.edu/law/journals-archive/bulr/documents/frankel.pdf. See also Deborah A. DeMott, Causation in the fiduciary realm, Boston University Law Review, 2011, Vol. 91, pp. 851-871, at p. 871.

[293] Frank H. Easterbrook & Daniel R. Fischel, Contract and Fiduciary Duty, id, at p. 432, mentioning, amongst others, trustee/beneficiary, pension trustee/beneficiary, guardian/ward, attorney/client, partner/partner, corporate manager/investor or lender/borrower. See also Tamar Frankel, Fiduciary Law, id, at p. 795 (mentioning that fiduciaries appear in a variety of forms, including agents, partners, directors and officers, trustees, executors and administrators, receivers, bailees, and guardians); D. Gordon Smith, The Critical Resource Theory of Fiduciary Duty, Vanderbilt Law Review, Vol. 55, pp. 1399-1497, at p. 1412-1413, mentioning that there can be formal fiduciary or informal fiduciary relationships; the former are those well-settled cases (e.g. trustee-beneficiary or attorney-client), where fiduciary duties apply as a matter of course, while the latter, often referred to as confidential relationships, are those in which the courts impose fiduciary duties based on a qualitative evaluation of the relationship.

[294] As Stout points out, the keystone of the duty of loyalty is the legal obligation that the fiduciary uses her powers not for her own benefit but for the exclusive benefit of the beneficiary; it is highly improper for a fiduciary to extract personal benefit from her fiduciary position without the beneficiary's consent, even when she may do this without harming the beneficiary. Lynn Stout, On the Export of U.S.-Style Corporate Fiduciary Duties to Other Cultures: Can a Transplant Take? (May 21, 2002), UCLA, School of Law, Working Paper No. 02-11 (available at https://ssrn.com/abstract=313679 or http://dx.doi.org/10.2139/ssrn.313679), pp. 1-39, at p. 14.

duties going beyond mere fairness and honesty. They could be obliged to act to further people's best interests[295].

And there would be many advantages that flexible[296] fiduciary laws could guarantee. Individuals could choose among alternative fiduciaries[297] and negotiate the terms of the relation, while the fiduciaries would rarely have monopoly over the people's needs; unless the individual agreed, the firm would not manipulate the terms of its performance[298]. Perhaps, individuals would know what information would be disclosed and could better understand processing techniques. Firms could also be obliged to consult[299] with individuals and give them the opportunity to express their best interests, or even opinions, in accordance with which data would be shared. Maybe, firms would implement internal policies and other safeguards or sign contracts to forbid e.g. re-identification of anonymized data. If this were the case, trust would be enhanced and, thus, data would be safely disclosed for the benefit of both firms and humans.

This way, the aspect of the lost control and the lack of secrecy[300] could be addressed, since the data subject would be capable of negotiating, choosing, determining, or (re)defining what information would be shared, by whom it would be processed, and under what specific circumstances[301].

Besides, in contrast to contract or status relations, where both parties seek to satisfy their needs, fiduciary relations are designed not to satisfy both parties' needs, but only those of the entrustor[302], who

---

[295] Deborah A. DeMott, Beyond Metaphor: An analysis of fiduciary obligation, Duke Law Journal, 1988, pp. 879-924, at p. 882, mentioning that "[…] *The fiduciary's duties go beyond mere fairness and honesty; they oblige him to act to further the beneficiary's best interests* […]".

[296] Ethan J. Leib, Friends as Fiduciaries, id, at pp. 707, 732 (arguing for the flexibility of fiduciary laws).

[297] In fact, fiduciary relations are not mandated by law. Floyd Mechem, Elements of the law of partnership, 2nd edition, 1920, Chicago Callaghan and Company, at p. 7, paragraph 5, mentioning that the law does not choose partners for people. However, once fiduciary relations are established, their legal consequences are determined by the law and the parties cannot waive the courts' supervision over the fiduciary. Alison Grey Anderson, Conflicts of Interest: Efficiency, Fairness and Corporate Structure, UCLA Law Review, 1978, Vol. 25, pp. 738-795, at p. 756 (see also at pp. 757-761, where several characteristics of the fiduciaries are mentioned).

[298] Tamar Frankel, Fiduciary Law, id, at p. 801.

[299] J. Sandberg, Socially Responsible Investment and Fiduciary Duty: Putting the Freshfields Report into Perspective, Journal of Business Ethics, 101, Springer 2010, pp. 143-162, at p. 145. Available at https://link.springer.com/content/pdf/10.1007%2Fs10551-010-0714-8.pdf.

[300] For instance, the courts would examine whether the individuals' consent was informed and independent. *William C. Rowland v. William H. Kable And Others*, Supreme Court of Virginia, 174 Va. 343, 6 S.E. 2d 633 (1940).

[301] Besides, as already argued, there is no choice to opt-out of data processing, while a hypothetical opt-out would mean opting-out of society. So, there is no choice but to entrust the processors "*with some matters where constant checking on performance is impractical*". And such situations are those where fiduciary laws apply. Annette C. Baier, Trust and Antitrust, Moral Prejudices: Essays on Ethics, id, at p. 139. Besides, superiority and asymmetry are demanded to establish a fiduciary relationship. Ethan J. Leib, Friends as Fiduciaries, id, at pp. 705, 721. And in the Big Data environment data processing practices can be regarded as the source of the requisite superiority and asymmetry.

[302] Tamar Frankel, Fiduciary Law, id, at p. 801, mentioning that an entrustor "*does not owe the fiduciary anything by virtue of the relationship*" (see also at pp. 818-819, mentioning that fiduciary relations do not create reciprocal legal obligations, "[…] *in contrast to contract and status law, a salient feature of fiduciary law is that it regulates only one of the parties – the fiduciary* […]").

may also monitor[303] fiduciaries[304]. In this context, affirmative duties to disclose[305] information could also be introduced to ensure that decisionmakers[306] would become accountable[307]. And how could accountability be achieved?

Accountability[308] refers to the extent to which decisionmakers are expected to justify their choices to those affected by these choices or to be held responsible[309] for their failures and wrongdoings[310]. Mechanisms of accountability could be supported by a model that would include transparency, due process, and justification. Namely, transparency could be enhanced as an incentive[311] for fair and efficient policies[312], since transparent decision-making exposes decisionmakers to the risk of

[303] Fiduciary law is in place to avoid having the beneficiary "*looking over the fiduciary's shoulder*". Kenneth B. Jr. Davis, Judicial Review of Fiduciary Decisionmaking - Some Theoretical Perspectives, Northwestern University Law Review, March 1985, Vol. 80, No. 1, pp. 1-99, at p. 6.

[304] For example, in case *Dodge et al. v. Ford Motor Co. et al.*, the court found that the price reduction, which Ford had declared for "the benefit of society" was an inappropriate act. The "donation" was an indeterminate amount to an unspecified number of unknown receivers; if the firm had been allowed to reduce prices as a gift to society both courts and the minority shareholders would have lost their ability to control the amount of the donation and its purpose. *Dodge et al. v. Ford Motor Co. et al.*, 204 Mich. 459, 170 N.W. 668 (1919).

[305] Robert C. Clark, Agency Costs versus Fiduciary Duties, in John W. Pratt & Richard J. Zeckhauser (eds), Principals and Agents: The Structure of Business, Harvard Business School Press, 1985, at p. 72 (see also at pp. 71-76, where Clark observes that affirmative duties to disclose, open-ended duties to act, closed-in rights to positional advantages, and moral rhetoric are common to fiduciary relations); Frank H. Easterbrook, Daniel R. Fischel, Contract and fiduciary duty, id, at p. 445; Scott FitzGibbon, Fiduciary Relationships Are Not Contracts, Marquette Law Review, Vol. 82 (Winter 1999), No. 2, pp. 303-353, at 308, mentioning that the fiduciary has an especially high duty to disclose: "*he is obliged to 'volunteer' information*".

[306] Fiduciaries are typically decisionmakers, whose specialized function is that of recommending or making decisions of a discretionary nature about the management or investment of the (property or) power of others. Alison Grey Anderson, Conflicts of Interest: Efficiency, Fairness and Corporate Structure, id, at p. 757.

[307] Some have used the term "responsibilization" to refer to the fact that technology is increasingly made responsible for decision-making. Rosamunde van Brakel, Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing, id, at p. 123 (citing David Garland).

[308] Traditionally, attention is drawn to formal accountability with regard to the branches of the government. Jody Freeman, The private role in public governance, New York University Law Review, 2000, Vol. 75, No. 3, pp. 543-675, at p. 549, arguing that accountability is more plural and contextual than traditional administrative law theory allows. Available at http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-75-3-Freeman_0.pdf.

[309] As some have argued, trust needs to be established to "*cede responsibility*" to systems. Adam Fusco, Ethics and Tech: A marriage made in heaven, or a divorce doomed in cyberspace? in Business Credit, March 2017, Vol. 119, No. 3, pp. 16-19, at p. 19.

[310] Michael W. Dowdle, Public accountability: Conceptual, historical and epistemic mappings, in MW Dowdle (ed.), Public Accountability: Designs, Dilemmas and Experiences (2006, Cambridge: Cambridge University Press), pp. 197-215, at p. 199. Available at http://press-files.anu.edu.au/downloads/press/n2304/pdf/ch12.pdf.

[311] Mark Fenster, The Opacity of Transparency, Iowa Law Review, 2006, Vol. 91, pp. 885-949, at pp. 894-901, arguing for transparency's benefits. Available at https://scholarship.law.ufl.edu/facultypub/46/.

[312] To some, transparency is essential to promote accountability and provide the public with a way to ensure that officials are not engaging in abuse. Daniel J. Solove, Nothing to Hide, id, at p. 193 (citing Justice Brandeis and James Madison).

"shaming"[313]. This way, fiduciaries could be exposed and entrustors would ensure that the former are not engaging in abuse. Due process[314] could enable the entrustor to challenge fiduciary's decisions; for instance, technological due process[315] would demand fiduciaries to satisfy some standards and confirm their fairness. Finally, accountability could be achieved by allowing public oversight; public review would require adequate explanation and justification accompanied by mechanisms[316] for sanctions[317].

This way, a new environment would emerge, where firms and natural persons could enjoy the chance to dance together; and they would do so with good reason, and, more importantly, for the benefit of human kind. Such an environment could perhaps address the aspect of the unequal[318] distribution of data's value.

And the fact that fiduciary relations can arise in the absence of contracts[319] could probably address the aspect of otherness; individuals, who would not be parties to contracts but who would be affected and influenced by data processing, would enjoy protection[320].

---

[313] Tal Z. Zarsky, Transparent Predictions, University of Illinois Law Review, Vol. 4, 2013, pp. 1503-1570, at p. 1534, arguing that transparency facilitates shaming. Available at https://www.illinoislawreview.org/wp-content/ilr-content/articles/2013/4/Zarsky.pdf.

[314] See, in general, Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, id.

[315] Danielle Keats Citron, Technological Due Process, Washington University Law Review, 2008, Vol. 85, No. 6, pp. 1249-1313, at p. 1301. Available at https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview.

[316] Besides, fiduciary laws provide several mechanisms for remedies, such as disgorgement, restitution, and paying a fair price to the beneficiary. Eileen A. Scallen, Promises Broken v. Promises Betrayed: Metaphor, Analogy, and the New Fiduciary Principle, University of Illinois Law Review, 1993, No. 4, pp. 897-980, at p. 912; Larry E. Ribstein, Are Partners Fiduciaries? University of Illinois Law Review, Symposium Issue, Vol. 2005, No. 1, February 2005, Illinois Public Law Research Paper No. 04-20, University of Illinois Law & Economics Research Paper No. LE04-008, pp. 101-140, at p. 111-112; Hanoch Dagan, The Law and Ethics of Restitution, Cambridge University Press, 2004 (published online 2009), at pp. 167-183.

[317] See Jennifer Shkabatur, Transparency With(out) Accountability: Open Government in the United States, Yale Law and Policy Review, 2012, Vol. 31, Issue 1, pp. 79-140, at p. 82, mentioning that "[…] *Public accountability consists of two components: the explanation and justification of agencies' activities to the public; and an accompanying mechanism for public sanctions* […]". Available at https://ylpr.yale.edu/sites/default/files/shkabatur_transparency_without_accountability-_open_government_in_the_united_states.pdf .

[318] Fiduciary laws are focused upon relationships of inequality. Leonard I. Rotman, Fiduciary Doctrine: A Concept In Need Of Understanding, Alberta Law Review, Vol. XXXIV, No. 4, 1996, pp. 821-852, at pp. 842-844; Ethan J. Leib, Friends as Fiduciaries, id, at p. 722; Paul B. Miller, A Theory of Fiduciary Liability, McGill Law Journal, Vol. 56, Issue 2, Feb. 2011, pp. 235-288, at para. 32; William Flanagan, Fiduciary duties in commercial relationships: When does the "commercial" become the personal?, in Law Commission Of Canada (ed.), Personal Relationships of Dependence and Interdependence in Law, 2002, pp. 57-77, at p. 69.

[319] Graham Douthwaite, Profits and Their Recovery, Villanova Law Review, 1970, Vol. 15, pp. 346-413, at p. 360 with further references; *Harrop v. Cole*, 85 N.J. Eq. 32, 95 A. 378 (Ch. 1915), *aff'd*, 86 N.J. Eq. 250, 98 A. 1085 (1916); Ethan J. Leib, Friends as Fiduciaries, id, at p. 677 ("[…] *fiduciaries need not necessarily be bound by contracts* […] *so the duty of good faith* […] *could add substance to the duties of the fiduciary outside of the contractual portion of their relationship with their beneficiaries* […]"). Besides, it would be impossible for parties to specify their duties in contracts, since the scope of fiduciary relationships is too complex and it involves details that they would not negotiate well. Robert Cooter & Bradley J. Freedman, The Fiduciary Relationship: Its Economic

Besides, a trust approach would very likely have a symbolic value as a statement of societal expectations[321]. This could have further advantages over the property-like approach; it would avoid the trap of alienability and the perverse incentives that a market in alienable personal data would create. After all, it would be fair to argue that what we need today is the emergence of societies based on fiduciary relations[322], whose moral[323] theme[324] includes loyalty, fidelity, faith[325] and honor[326]. So, maybe, the law should provide incentives to encourage potential fiduciaries and entrustors to enter into such relations, which by law demand fairness.

Since the more powerful the algorithm, the more powerful the firms, the latter could be regarded as data-fiduciaries. They do have special power over others and special relationship to others; What if Airbnb used its data to embarrass politicians and what if an attorney-at-law or a physician sold their clients' personal data to brokers? The duty of loyalty and trustworthiness would probably ensure that the fiduciary would act in the interest of the beneficiary; the entrusted fiduciary would not betray the trust. Since, in almost every case, these potential data-fiduciaries hold sensitive data, it seems that they should have a duty of care, a duty to act competently and diligently. Besides, professionals, having skills and knowledge, and individuals, being ill-prepared to monitor fiduciaries' behavior and to prevent them from abusing data, are not equal. And this leads to asymmetry, a prerequisite for

---

Character and Legal Consequences, id, at p. 1048, mentioning that in fiduciary relationships the parties are unable to foresee the conditions under which one act produces better results than another.

[320] Namely, a trustee has a duty to comply with the terms of the trust instrument, even though the beneficiary is not a party to that instrument. Tamar Frankel, Fiduciary Law, id, at p. 825.

[321] Humankind needs trust as a foundational good for societal organization and survival; and trust is "*a notoriously vulnerable good, easily wounded and not at all easily healed*". Annette C. Baier, Trust and Antitrust, Moral Prejudices: Essays on Ethics, id, at p. 130.

[322] The understanding and implementation of fiduciary duties are dynamic and constantly evolving in response to changes in society, economy, and knowledge. The European Commission, Resource Efficiency and Fiduciary Duties of Investors, id, at p. 22; Kenneth M. Rosen, Fiduciaries, Meador Lecture Series 2005-2006: Fiduciaries, Alabama Law Review, Vol. 58, pp. 1041-1048, at p. 1042 ("[…] *Notions of fiduciaries and their duties continue to permeate the law* […] *Their importance only continues to grow* […]").

[323] Courts often "express" themselves as if they are importing moral requirements into the law through their policing of fiduciary relationships. This way, courts draw from the moral sphere, use informal social norms to influence fiduciary behavior, and create extra-legal norms. Elizabeth S. Scott and Robert E. Scott, Parents as Fiduciaries, id, at pp. 2422, 2425 ("[…] *The stance of moral neutrality that courts adopt toward efficient breach in other contexts is absent here; fiduciary default is treated as a moral violation with attendant reputational costs* […]"); Larry E. Ribstein, Are Partners Fiduciaries?, id, at p. 127 ("[…] *the strong language in judicial opinions* […] *arguably help*[s] *create extra-legal norms* […]"); Robert Cooter & Bradley J. Freedman, The Fiduciary Relationship: Its Economic Character and Legal Consequences, id, at pp. 1073-1074 ("[…] *Disloyalty brings moral condemnation* […] *The ponderous language of moral censure in fiduciary cases can wound the defendant* […] *An allegation of breach of fiduciary duty carries with it the stench of dishonesty-if not of deceit, then of constructive fraud* […]").

[324] Admittedly, the standards for good faith, loyalty and similar values would better derive from ethics and morality, rather than the marketplace. It might be abnormal, inefficient, and, perhaps, dangerous to implement marketplace-or-property-like approaches and introduce them as the baseline and background for privacy and personal data protection.

[325] Scott FitzGibbon, Fiduciary Relationships Are Not Contracts, id, at p. 309, mentioning that the fiduciary's duty of good faith is stronger than that which applies in commercial arrangements generally.

[326] See, e.g., *Henley v. Birmingham Trust National Bank*, 322 So. 2d 688 (1975), SC 780, Supreme Court of Alabama (1975). As some have argued, the moral behavior of fiduciaries is altruistic, voluntary, and related to the vulnerability of the entrustor. Tamar Frankel, Fiduciary Law, id, at pp. 829-832, discussing the moral theme in fiduciary regulation.

fiduciaries laws to apply. In the relationship between users and firms, one can detect vulnerability, dependence, and the experts' awareness of possessing valuable information. The above could justify the implementation of fiduciary laws. And it would be feasible that those, not being parties to contracts but still being affected by their data processing, could enjoy protection.

But, at this point, one should also consider what duties of good faith and ethical conduct in processing are owed to the members of the society as a whole. So, in addition to the above values that fiduciary laws would ensure and since anything on the Internet can be regarded as fair game[327], could duties of fair play be added?

[327] Adam Fusco, Ethics and Tech: A marriage made in heaven, or a divorce doomed in cyberspace?, id, at p. 17.

Chapter VI. Fair Play

Fair play[328] is the fair[329] and honest treatment of people[330]; the respect for the rules or the equal treatment of all concerned[331].

The Internet has created virtual worlds[332], where fantasy and play[333] blend together and create an everyday "entertaining" existence. And this is not a game we choose, it is one we are forced to play;

[328] Johan Huizinga, Homo Ludens: A Study of the Play-Element in Culture, Routledge & Kegan Paul, London, Boston and Henley, 1944, at pp. 211-212, "[…] *Civilization will, in a sense, always be played according to certain rules, and true civilization will always demand fair play* […] *Fair play is nothing less than good faith expressed in play terms* […] *the cheat or the spoil-sport shatters civilization itself. To be a sound culture creating force this play-element must be pure. It must not consist in the darkening or debasing of standards set up by reason, faith or humanity. It must not be a false seeming, a masking of political purposes behind the illusion of genuine play-forms. True play knows no propaganda; its aim is in itself, and its familiar spirit is happy inspiration* […] *Life must be lived as play* […]"). To Rawls, the principle of fair play can be defined as follows: Suppose that there is a beneficial and just scheme of social corporation and that the advantages it yields can only be obtained if everyone cooperates; then, suppose that this cooperation requires some sacrifice from each person, or at least involves some restriction of her liberty; finally, suppose that the benefits produced by that cooperation are free. In this context, a person who has accepted the benefits of the scheme is bound by a duty of fair play to do her part and not to take advantage of the free benefit by not cooperating. And the reason one must abstain from this attempt is, to Rawls, that the existence of the benefit is the result of everyone's effort; it belongs, in fairness, to no one. John Rawls, Legal Obligation and the Duty of Fair Play, in Collected papers, Rawls & Freeman, Harvard University Press, 2001, pp. 117-129, at pp. 122-123 (formerly published in Law and Philosophy, S. Hook (ed.), New York: New York University Press, 1964). So, in the above situation, there must be an active scheme of social cooperation; cooperation has to involve at least a restriction of one's liberty; and the benefits yielded by the scheme may be received in, at least, some cases by someone who does not cooperate when her turn comes. John Simmons, The Principle of Fair Play, Philosophy and Public Affairs, Vol. 8, No. 4 (Summer, 1979), pp. 307-337 (formerly published by Princeton University Press), at pp. 310, 314, 315 (mentioning that the justice condition on this argument, serves the purpose of assuring that a man is bound to do his fair share only if he is allocated a fair share of benefits and accepts some of them). But see Robert Nozick, Anarchy, State, and Utopia, New York, Basic Books, 1974, at p. 93, arguing against the principle of fairness.

[329] Arthur Dobrin, It's Not Fair! But What Is Fairness? Three different ideas of fairness: sameness, deservedness, and need, May 11, 2012, Psychology Today (available at https://www.psychologytoday.com/intl/blog/am-i-right/201205/its-not-fair-what-is-fairness), arguing that there are three ideas about fairness: sameness (meaning there is fairness where everything is equal); deservedness (i.e. one gets what she deserves); and need (that is those who have more to give should give a greater percentage of what they have to help others who are unable to contribute much). See also Danah Boyd, What is "fairness"? What happens when technology decides? The Message, Sep 3, 2014 (available at https://medium.com/message/what-is-fairness-73940071840), mentioning that "*the most important thing that we all need to recognize is that how fairness is instantiated significantly affects the very architecture of our society*".

[330] Cambridge dictionary: https://dictionary.cambridge.org/dictionary/english/fair-play.

[331] Oxford dictionary: https://en.oxforddictionaries.com/definition/fair_play.

[332] Raph Koster, Declaring the rights of players, in Salen & Zimmerman (eds), The Game Design Reader, 2000, pp. 788-812 (available at https://com427fall2013ncsu.files.wordpress.com/2013/08/koster-2006-declaring-the-rights-of-players.pdf or https://www.raphkoster.com/games/essays/declaring-the-rights-of-players/).

opting-out would not be a realistic choice. But a game should not involve a moral consequence; the only moral consequence that may happen is the very act of ending the game[334]. So, a game could be regarded as a place where we only act as if something matters[335], albeit we need play[336] to bring order[337] in everyday life. People in the Internet ought to be treated as people, while codes and laws should promote well-being and respect human dignity to the greatest extent possible[338].

In the past, fantasy was implemented into laws to create fictional persons and solve people's problems. Namely, when laws certify the existence of "Lessig, Inc.", we all play a game and pretend[339] that "Lessig" has nothing to do with "Lessig, Inc."[340]. And the benefit of having fantasy-corporations became apparent to society; there are no objections that we needed the law. The game of make-believe was not fun; it was useful and it led to societal benefits and economic growth.

---

[333] Koen B. Tanghe, Homo Ludens (1938) and the crisis in the Humanities, in Cogent Arts & Humanities, 2016, Vol. 3 (1245087), http://dx.doi.org/10.1080/23311983.2016.1245087, pp. 1-15, at p. 1 ("[…] *Cultures arise and unfold in and as play but* […] *they tend to lose their playfulness as they mature* […]").

[334] Johan Huizinga, Homo Ludens: A Study of the Play-Element in Culture, id, at pp. 6-8, 28, mentioning that play "*has no moral function*"; it is never imposed by physical necessity or moral duty; it is never a task; it is a voluntary activity; "[p]*lay to order is no longer play*".

[335] Play is free but it is not real; it is rather stepping out of real life; "[e]*very child knows perfectly well that he is "only pretending"*". But the consciousness of play being only a pretend does not prevent it from "*proceeding with the utmost seriousness*". Johan Huizinga, Homo Ludens: A Study of the Play-Element in Culture, id, at p. 8.

[336] Johan Huizinga, Homo Ludens: A Study of the Play-Element in Culture, id, at p. 3 ("*Play cannot be denied. You can deny* […] *justice, beauty, truth, goodness, mind, God* […] *seriousness, but not play* […]").

[337] Play creates order; it is order. Johan Huizinga, Homo Ludens: A Study of the Play-Element in Culture, id, at pp. 10-11, mentioning that "[i]*nto an imperfect world and into the confusion of life* [play] *brings a temporary, a limited perfection*" and as soon as the rules are transgressed the whole play-world collapses; the game is over.

[338] See, in general, Lawrence Lessig, Code, Version 2.0, id.

[339] As regards pretending, some authors have argued that we are far from the only dishonest species, but we are surely the most dishonest "*if only because we do the most talking*". David Brin, The Transparent Society, id, at p. 120, citing Robert Wright (The Moral Animal: Why We Are the Way We Are: The New Science of Evolutionary Psychology, New York, Pantheon, 1994).

[340] Central to the debate who or what is a "person" in law is whether the legal person must "approximate a metaphysical person". Ngaire Naffine, Who are Law's Persons? From Cheshire Cats to Responsible Subjects, in The Modern Law Review Limited, 2003, Vol. 66, No. 3, Blackwell Publishing Ltd, pp. 346-367, at pp. 346, 350 (mentioning that there are three types of legal persons: P1, P2 and P3; "[…] *P1 theorists* […] *reject the claim that legal personality* […] *builds upon a metaphysical conception of the person. P2 theorists* […] *assume that humanity, rather than the narrower conception of personhood, is the basis of both moral and legal claims on others and the basis of legal personality. P3 theorists* […] *invoke metaphysical persons, variously understood* […] *but then their definition of the person cannot be said to represent the official legal view of personality* […]"). See also Elvia Arcelia Quintana Adriano, The Natural Person, Legal Entity or Juridical Person and Juridical Personality, The Penn State Journal of Law & International Affairs, 2015, Vol. 4, Issue 1, Seventeenth Biennial Meeting of the International Academy of Commercial and Consumer Law, pp. 363-391, at p. 366 ("[…] *A person is juridically classified in two groups: natural persons and juridical persons. The first group refers to a human being, who is an individual being capable of assuming obligations and capable of holding rights. The second group refers to those entities endowed with juridical personality who are usually known as a collective person, social person, or legal entity* […]").

So, why not pretend[341] that these virtual worlds, created by the Internet, are places of fairness[342]? Places that would allow everyone to live in worlds where magic would be real?

Perhaps, we could rely on data scientists, those who are able to design systems in ways that would benefit humanity and protect people's fundamental rights. Implementation of several principles into the very design specifications of systems could be promoted to embed trust and transparency rules within data processing and analyzing procedures[343]. Tools could be used to keep systems user-centric[344] and lessons could be learnt from several fields, where similar approaches have been conducted to

[341] Besides, the term "person" comes from the Latin "persona" (meaning "role") or, to some, the Etruscan "phersu" (actor's mask). See, amongst others, Jessica Clark, Humm Coudry, Praeda. Butin de guerre et société dans la Rome républicaine, The Classical Review, Cambridge, Vol. 61, Issue 2, Oct. 2011, pp. 549-551, at p. 549; Jorg Kustermans, The category rogue, Thesis Eleven, Vol. 114, No. 1, pp. 3-14, at p. 9.

[342] As regards fair information principles, see William Bonner & Mike Chiasson, If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy, Information and Organization, 2005, Vol. 15, pp. 267-293, at pp. 275-276; OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 (proposing eight fair information principles as regards personal data: Collection Limitation Principle; Data Quality Principle; Purpose Specification Principle; Use Limitation Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; and Accountability Principle); HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems, Records, computers, and the Rights of Citizens, The Code of Fair Information Practices, 1973, (mentioning that there must be no personal data record-keeping systems whose existence is secret; there must be a way for an individual to find out what information about the person is in a record and how it is used; there must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent; there must be a way for a person to correct or amend a record of personal data; any organization creating, maintaining, using, or disseminating records of personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses), available at https://www.epic.org/privacy/consumer/code_fair_info.html. As regards fair online economy, the International Cooperative Alliance has proposed the following principles: voluntary and open membership; democratic member control; member economic participation; autonomy and independence; education, training and information; cooperation among cooperatives; and concern for community. These could be accompanied by values of self-help, self-responsibility, democracy, equality, equity and solidarity. See ICA's website (https://www.ica.coop/en/whats-co-op/co-operative-identity-values-principles); Nathan Schneider, An Internet of ownership: Democratic design for the online economy, The Sociological Review Monographs, 2018, Vol. 66, No. 2, pp. 320-340, at pp. 323-324.

[343] Similarly, the principle of Privacy by Design (PbD) has been established to guarantee that privacy and data protection are embedded within the "*entire life cycle of the technology, from the very early stage, right through to their ultimate deployment, use and ultimate disposal*". Article 25 of the GDPR; Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 2010/C 280/01, at paragraph 19. See also the seven principles proposed by Cavoukian in Ann Cavoukian, Privacy by Design, The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, available at http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf.

[344] Besides, "permissionless innovation" cannot be a synonym for unaccountability. John Daley, Insecure Software Is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-Embedded Systems, Stanford Technology Law Review, Spring, 2016, Vol. 19, No. 3, at p. 533. Available at https://law.stanford.edu/publications/insecure-software-is-eating-the-world-promoting-cybersecurity-in-an-age-of-ubiquitous-software-embedded-systems/.

implement fair information principles into technologies[345]. Namely, in fields of biometrics[346], encryption has been proposed to put control over biometric data in the hands of the individuals and enhance their confidence[347] towards the system[348]. In fields of e-Health[349], emerging devices have been designed to capture the minimum data required[350]. And in fields of surveillance techniques, smart cameras have been proposed to avoid discriminatory targeting[351].

Maybe, by implementing fair information principles into the very heart-design-specifications and the entire life cycle of systems, negative effects could be avoided, fairness would be enhanced, and, hence, magic would be real.

[345] Anna Romanou, The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise, Computer Law & Security, 2018, Vol. 34, pp. 99-110, at pp. 104-108.

[346] Biometrics can be defined as the technology that uses automatic personal recognition based on psychological or behavioral characteristics. Ruud Bolle, Sharath Pankanti, Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society, Anil K. Jain (ed.), Kluwer Academic Publishers Norwell, MA, USA, 1998. Any human trait may be regarded as biometrics as long as it is universal (meaning every human being possesses it), distinctive (i.e. unique), permanent (i.e. it remains invariant for some period of time), and quantitatively measurable (meaning certain quantity is needed to be measurable). S. Prabhakar, S. Pankanti, A.K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security & Privacy, Vol. 99, Issue: 2, Mar-Apr 2003, pp. 33-42. See also Article 4(14) of the GDPR.

[347] Besides, confidentiality (meaning hiding information to outsiders) has, historically, been the primary goal of cryptology (i.e. the science of dealing with the protection of information and computation using mathematical techniques). David Kahn, The Codebreakers: The Story of Secret Writing, 1967, The Macmillan Company, New York, available at http://mindguruindia.com/wp-content/uploads/2014/06/MP069_The-CodeBreakers.pdf.

[348] The European Commission, Putting privacy at the heart of biometric systems, 18 August 2011, available at https://ec.europa.eu/digital-single-market/en/news/putting-privacy-heart-biometric-systems; A. Cavoukian, A. Stoianov, Privacy by Design Solutions for Biometric One-to-Many Identification Systems", IPC Technical Report, June 2014, available at https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf.

[349] E-Health can be understood as an emerging field in the intersection of medical informatics, public health, and business that refers to services and information delivered and enhanced through the Internet and similar technologies. Eysenbach regards e-Health as a commitment for global thinking to improve healthcare both locally and worldwide. G. Eysenbach, What is e-health?, Journal of Medical Internet Research, 2001, Vol. 3, No. 2, doi:10.2196/jmir.3.2.e20, available at http://www.jmir.org/2001/2/e20/.

[350] Take, for instance, Intel's device to better connect clinicians with patients at https://www.intel.com/pressroom/archive/releases/2008/20081110corp.htm; http://web.nchu.edu.tw/pweb/users/arborfish/lesson/7736.pdf; http://thefutureofthings.com/6259-intel-health-guide/.

[351] Andrea Cavallaro, Privacy in Video Surveillance, IEEE Signal Processing Magazine, March 2007, at p. 166, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4117949.

Chapter VII. Conclusions & Discussion

So far, it has been argued that it is data fiduciaries and fair play that could most probably be introduced to address the personal data protection problem. It seems that a property-like approach would not be sufficient: while promising moral rights would be capable of addressing several aspects of the problem, albeit they are not supposed to function as commodities; a *sui generis* rights approach would lead to uncertainties, and trade secrecy rights would not be asserted against those who process data, albeit are not in privity with the individual.

On the other hand, fiduciary laws seem to achieve the optimal result. Maybe, such flexible laws would address the four aspects of the data protection problem. They could strengthen the individuals' control over their information, protect the secret nature of data, equally distribute their value, and, in the absence of contracts and in conjunction with fair play, address the aspect of otherness. Establishing trust and fair play would very likely guarantee the respect and the magic that members of any society need and deserve. In this context, discussion needs to mature and take trust seriously to work towards responsible ways of generating societal value out of data.

But there is one last approach, which needs to be examined; a technological approach and, in particular, promising blockchains.

Some state that new technologies can mathematically provide trust in a network that is the very trusted party, overseeing and auditing the proper completion of transactions[352]. And they promise that people will enjoy trustworthiness in systems, where each element, being fully dynamic and not tied to specific physical space, will not be managed as a physical object (e.g. with an owner)[353].

Relying on existing centralized systems is costly. Namely, relying on a bank requires banking fees. And this may increase inequality; not all people have a bank account. So, firms and organizations[354] are looking to use blockchain[355] to overcome such problems[356].

---

[352] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at https://bitcoin.org/bitcoin.pdf, pp. 1-9.

[353] Take, for example, Ethereum that is said to provide a system for running a decentralized application platform. Vitalik Buterin, Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application Platform, 2014, available at https://coss.io/documents/white-papers/ethereum.pdf. Interestingly, this brings real-world challenges to cyberspace (e.g. where do we pay taxes for this service or under what jurisdiction does it fall?).

[354] In fact, blockchain technology has been embraced by start-ups, financial institutions and technology firms. See, amongst others, Digital asset holding (https://www.digitalasset.com/); Stellar (https://www.stellar.org/); Ripple (https://ripple.com/); Yessi Bello Perez, 8 Banking Giants Embracing Bitcoin and Blockchain Tech, Coindesk, July 27, 2015, available at https://www.coindesk.com/8-banking-giants-bitcoin-blockchain/; IBM (https://www.ibm.com/blockchain).

[355] Some regard blockchain technology as a tool that will influence business and society in the years to come. Amy Webb, 8 Tech Trends to Watch in 2016, Harvard Business Review, December 8, 2015, available at https://hbr.org/2015/12/8-tech-trends-to-watch-in-2016. To others, this disruptive technology is to support information exchange and transactions that demand authentication and trust. Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, Where Is Current Research on Blockchain Technology? - A Systematic Review, 2016, PLoS ONE 11(10), e0163477, doi: 10.1371/journal.pone.0163477, available at http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0163477&type=printable, pp. 1-27,

Blockchain is said to be a sophisticated and distributed[357] online ledger[358]. To some, it is the distributed trust network that the Internet always needed and never had[359]. As many authors argue, blockchain allows people, who have no confidence in each other, to collaborate without having to go through a neutral central authority[360]; to others, it is a machine for creating trust[361], or a shared, trusted, and public ledger that anyone can inspect but that no single user controls[362].

---

at p. 2, mentioning that blockchain still has some technical challenges and limitations that need to be addressed.

[356] For instance, the U.S. Defense Advanced Research Projects Agency (DARPA) is looking to use blockchain to create an unhackable messaging system. Naomi Lachance, Not Just Bitcoin: Why The Blockchain Is A Seductive Technology To Many Industries, NPR, May 4, 2016 (available at https://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries?t=1530943746094). To some, blockchain has already disrupted some industries. Nir Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommunications Policy, 2017, Vol. 41, pp. 1027-1038, at p. 1030; Mauro Conti & Sandeep Kumar, A Survey on Security and Privacy Issues of Bitcoin, 2017, available at https://arxiv.org/pdf/1706.00916.pdf; World Economic Forum, The future of financial infrastructure, An ambitious look at how blockchain can reshape financial services, 2016 (concluding that the blockchain will fundamentally alter the way financial institutions do business around the world).

[357] Blockchain technology is said to store same information at different nodes; storing transactions in different nodes is called a "distributed ledger". Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly 34, 2017, pp. 355-364, at p. 355.

[358] As some argue, a superior feature of blockchain is its decentralized, immutable, and auditable database for secure transactions with privacy protection. Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 2015, pp. 180-184.

[359] Brian Fung, Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today, Washington Post, May 21, 2014 (available at https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/?noredirect=on&utm_term=.14673fc41817).

[360] Authors argue that blockchain holds promise of reducing the costs of establishing and maintaining trust for individuals and organizations. Pim Otte, Martijn de Vos, Johan Pouwelse, TrustChain: A Sybil-resistant scalable blockchain, Future Generation Computer Systems, 2017, doi: 10.1016/j.future.2017.08.048, pp. 1-11, at pp. 1-2, mentioning that three distinct blockchain architectures have emerged: permission-less cybercurrency (ensuring that no middleman needs to be asked for permission, no identity provider needs to approve one's application, and no financial entity is required); private transaction fabric (where transactions are not exposed to all by default); and permission-less transaction fabric (like Ethereum, where general purpose programs are executed in permission-less settings, while, at the same time, scalability is maintained). All the above architectures aim to facilitate trustworthy transactions in scale. See Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer, On Scaling Decentralized Blockchains (A Position Paper), in Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, Kurt Rohloff (eds), Financial Cryptography and Data Security, FC 2016 International Workshops Bitcoin, Voting, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers, pp. 106-125; Florian Hawlitschek, Benedikt Notheisen, Timm Teubner, The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, Electronic Commerce Research and Applications, Vol. 29, May-June 2018, pp. 50-63, at p. 51. As some authors have argued, the main variants are either private or public closed blockchains (private/public permissioned) versus private or public open blockchains (permissionless); whether a ledger is public or private determines who has access to copies of the ledger; the attribute of permission versus permissionless determines who maintains the ledger. Michael Mainelli, Mike Smith, Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (Aka Blockchain Technology), November 7, 2015, Journal

As scholars have stated, one of its main features is consensus[363], meaning the blockchain algorithm enables distributed consensus on who owns what. It is said to be a proof of work, a proof of an action at a point in time. Blockchain is believed to use cryptographic signatures and public keys chain-linked to form an unforgeable record of transactions for e.g. digital cash or any ledger record; crypto-proof replaces the notary[364].

But could blockchain really ensure trust in systems?

---

of Financial Perspectives, 2015, Vol. 3, No. 3, available at https://ssrn.com/abstract=3083963; Government Office for Science, Distributed Ledger Technology: beyond block chain, A report by the UK Government Chief Scientific Adviser, 2016, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. It is argued that in permissionless blockchains (like Bitcoin), anyone can participate and anyone, who is willing to pay the fees, can create accounts and propose transactions; a lack of control over who can participate is often the goal of such systems. On the other hand, with regard to permissioned systems, authors state that participation is controlled by an authority; this helps comply with the "know your customer" regulation. Maurice Herlihy, Mark Moir, Blockchains and the Logic of Accountability: Keynote Address, LICS '16 Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, New York, USA, July 05-08, 2016, pp. 27-30, at p. 27.

[361] The Economist, The promise of the blockchain, The trust machine, The technology behind bitcoin could transform how the economy works (October 31, 2015), available at https://www.economist.com/leaders/2015/10/31/the-trust-machine (mentioning that blockchains are "*the latest example of the unexpected fruits of cryptography*").

[362] It has been stated that blockchain enables radical transparency a lot easier than it enables radical anonymity. Scott J. Shackelford & Steve Myers, Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace, The Yale Journal of Law and Technology, 2017, Vol. 19, pp. 334-388, at p. 356 (mentioning that people may be able to reach exactly those they wish to reach without invading their privacy; an idea called "black box marketing"); Cassie Findlay, Participatory cultures, trust technologies and decentralisation: Innovation opportunities for recordkeeping, Archives and Manuscripts, 2017, Vol. 45, No. 3, pp. 176-190, at p. 179 (who mentions that, in record keeping terms, blockchain technology creates a ledger or register that is shared by users and is owned and controlled by no one).

[363] Consensus has been defined as decision-making among participant nodes. Kim Shiho, Blockchain for a trust network among intelligent vehicles, id, at p. 23 (mentioning that "[…] *For a transaction to be valid, all participants must agree on the validity of a predefined algorithm or rule, such as proof-of-work, proof-of-stake, proof-of-concept, or else. The consensus involves conducting two key crucial functions of the blockchain technology. First, consensus protocols allow newly generated data block to be appended to a distributed ledger, while ensuring that every block in the chain is truly valid and keeping participants incentivized to do mining. It prevents malicious hackers* [from] *controlling or breaking down the blockchain system. Second, the consensus rule guarantees that a single blockchain keeps growing and is followed* […]").

[364] Jonathan Levin, I Love the Blockchain, Just Not Bitcoin, November 16, 2014, available at https://www.coindesk.com/love-blockchain-just-bitcoin/, who argues that blockchains are data structures with two distinct features: they have tokens that form the basis of all recorded information and economic incentives for using the system; they contain a chain of cryptographic proofs, ensuring the data have not been tampered with, so that the chain of proofs would not be able to be reconstructed ("[…] *The chain of proofs has the neat property that it reveals the amount of work it took to construct the chain* […] *This enables the network to converge on one chain as the true chain, the one with the most work done, and discard all but one* […]").

Record systems are trustworthy if they are reliable, accurate, and authentic[365]. As many authors argue[366], reliability can be understood as the trustworthiness of a record as a statement of fact, based on the competence of its author, its completeness, and the controls of its creation; accuracy can be defined as the correctness of the very content; and authenticity can be regarded as the trustworthiness of the record as a record, meaning that it is what it purports to be, free from tampering or corruption, based on the competence of its keepers through time.

Determining trust could be a matter of making a risk assessment; if the risk is low, it is probably possible to trust the object or artefact[367]. Duranti and Rogers[368] argue that this assessment could depend on four types of knowledge: reputation, resulting from the evaluation of the trustee's past actions; performance, i.e. the relation between one's present actions and the conduct required to fulfil her current responsibilities, as specified by the truster; competence, consisting of having the knowledge and skills to perform a task to any given standard; and confidence, i.e. assurance of expectation of action and conduct the truster has in the trustee.

A blockchain is said to differ from existing networks as regards how transactions occur and how data are stored and secured[369]. It can be understood as a distributed transaction database, in which different nodes cooperate as a system to store sequences of bits that are encrypted as a single unit or block and then chained together. Lemieux[370] provides an apt overview[371] of the process concerning Bitcoin[372]

---

[365] Luciana Duranti & Corinne Rogers, Trust in digital records: An increasingly cloudy legal area, Computer Law & Security Review, 2012, Vol. 28, pp. 522-531, at p. 525, mentioning that authenticity is composed of both identity and integrity, where "[…] *identity is the whole of the attributes of a record that characterize it as unique and distinguish it from other records* […] *and integrity is the quality of a record that is capable of transmitting exactly the message it is meant to communicate in order to achieve its purpose* […]".

[366] Bonnie Mak, On the Uses of Authenticity, Archivaria, 73, The Journal of the Association of Canadian Archivists, Spring 2012, pp. 1-17; Luciana Duranti, Diplomatics: New Uses for an Old Science, Archivaria, 28, The Journal of the Association of Canadian Archivists, Summer 1989, pp. 7-27. Reliability as a statement of fact begins with the process of creation, and authenticity deals with establishing and preserving the identity and the integrity from the creation and thereafter. Corinne Rogers, Virtual Authenticity: Authenticity of Digital Records from Theory to Practice, MAS, The University of British Columbia, 2015, available at https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0166169, at pp. 1, 34, 37, 191.

[367] Geoffrey Yeo, Trust and context in cyberspace, Archives & Records, 2013, Vol. 34, No. 2, pp. 214-234, at p. 215; Jens Riegelsberger, M. Angela Sasse, John D. McCarthy, The mechanics of trust: A framework for research and design, International Journal of Human-Computer Studies, Vol. 62, Issue 3, 2005, pp. 381-422, at p. 385 ("[…] *trust will only be required if there are things at stake and if there is the possibility of adverse outcomes* […]").

[368] Luciana Duranti & Corinne Rogers, Trust in digital records: An increasingly cloudy legal area, id, at p. 522 with further references.

[369] Eric Funk, Jeff Riddell, Felix Ankel, Daniel Cabrera, Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education, Journal of the Association of American Medical Colleges, DOI: 10.1097/ACM.0000000000002326, June 12, 2018, available at https://insights.ovid.com/crossref?an=00001888-900000000-97880, pp. 1-17, at pp. 3-4.

[370] Victoria Louise Lemieux, Trusting records: is Blockchain technology the answer?, Records Management Journal, 2016, Vol. 26, Issue 2, pp. 110-139, at p. 119.

[371] Similar overviews have been provided by other authors. Namely, as regards transactions, see, amongst others, Vitalik Buterin, Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application Platform, id. See also Eric Funk, Jeff Riddell, Felix Ankel, Daniel Cabrera, Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education, id, at pp. 3-4, describing the procedure as

blockchain[373]: X proposes the transfer of Bitcoin to Y; the network checks that there is sufficient Bitcoin in X's wallet; nodes (miners) bundle the proposal with other transactions[374] to create a new block[375]; the blocks are cryptographically hashed (i.e. they are used as input to an algorithm that converts them into an alphanumeric string: the "hash value"); the hash is put into the header of the proposed block; the header becomes the basis for the proof of work performed by the nodes on the network; when a node reaches a solution to the proof-of-work, other nodes check it and then each; the node that confirms the solution updates the blockchain with the hash of the header (of the proposed block); this becomes the new block's identifying string (and is part of the distributed ledger); the transaction is confirmed.

X pays Y.

Simply put, blockchain is a software solution protocol; it can be understood as children playing basketball: the game is successfully played in the absence of a referee, as all kids are aware of the rules and play according to them; all agree on the score, so there is no need for a score keeper; in case of a foul, children reach consensus and continue playing; no kid can change the rules, but any child may leave or join as long as she accepts the score and the rules[376].

---

follows: a blockchain network is created and an original block, the genesis block, serving as anchoring block, defines the type of data and transactions. Data is, then, recorded, if user A initiates a transaction to send information to user B; a different subset of network members ("miners") listen requests and record transactions into blocks, acting like "*freelance registrars who get compensated*". So, a block is a list of transactions and miners add the current block on to the growing list of blocks that have been recorded previously. Each block is, hence, chronologically linked ("chained") to the previous blocks.

[372] As some argue, Bitcoin has served as the basis for the implementation of blockchain in energy sector, supply chains, music industry, and healthcare. See, amongst others, Christoph Burger, Andreas Kuhlmann, Philipp Richard, Jens Weinmann, Blockchain in the energy transition, A survey among decision-makers in the German energy industry, Deutsche Energie-Agentur GmbH (dena) - German Energy Agency and ESMT European School of Management and Technology GmbH, Berlin, November 2016; Marco Iansiti, Karim Lakhani, The truth about blockchain, Harvard Business Review, Jan-Feb 2017, available at https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf; Rethink Music & Berklee Institute of Creative Entrepreneurship (Berklee ICE), Rethink Music: Transparency And Money Flows In The Music Industry, Recommendations to Increase Transparency, Reduce Friction, and Promote Fairness in the Music Industry, available at https://www.berklee.edu/sites/default/files/Fair%20Music%20-%20Transparency%20and%20Payment%20Flows%20in%20the%20Music%20Industry.pdf; Matthew Hoy, An Introduction to the Blockchain and Its Implications for Libraries and Medicine, Medical Reference Service Quarterly, 2017 (Jul-Sep), Vol. 36, No. 3, pp. 273-279 (doi: 10.1080/02763869.2017.1332261).

[373] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, id, at pp. 1-3.

[374] To some, "miners" is not an apt term to describe what these actors do. Stephen Williamson, Is Bitcoin a Waste of Resources?, Federal Reserve Bank of St. Louis Review, Second Quarter 2018, Vol. 100, No. 2, available at https://doi.org/10.20955/r.2018.107-15, pp. 107-115, at 107.

[375] Some regard blocks as time stamped batches of valid transactions. Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, id, at p. 356 (who also refer to mining as creating new blocks).

[376] Eric Funk, Jeff Riddell, Felix Ankel, Daniel Cabrera, Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education, id, at p. 5 (see also at p. 7, arguing that blockchain could lead to rapid, efficient, transparent, and explicit management of education instruments).

And blockchain does not, by its very construction, ensure trustworthiness, as the latter can only be guaranteed if the records are reliable and authentic. Blockchain does not address the very reliability of the records. Besides, a system is secure, if honest nodes collectively control more CPU power than any group of attacker nodes[377]; to modify a past block, the attacker would have to redo the proof-of-work and all blocks after it and then catch up with and surpass the work of honest nodes[378].

Blockchain is said to facilitate the exchange of value without the need of an intermediary[379]. It is also said to refer to a cryptographically secured distributed ledger with a decentralized consensus mechanism[380]. But how could a shift towards sharing platforms based on trust-free blockchains affect users' behavior in the developing platform landscape? Would the trust-machines be capable of disrupting[381] the trust business of a sharing economy[382]?

Blockchain's advantages are said to be decentralization, cost efficient micro-transactions[383], no complexity in writing contracts[384], and information sharing[385]. And its disadvantages are said to include: the fact that it is built on public availability of data and disclosure of transacting parties (and this could

[377] "[…] *For the system to work, it has to be more costly to cheat than for the correct information to be added in the new block* […]". Stephen Williamson, Is Bitcoin a Waste of Resources?, id, at pp. 107-108.

[378] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, id, at p. 3.

[379] Primavera De Filippi, What Blockchain Means for the Sharing Economy, 2017, Harvard Business Review, at p. 2 (available at https://bitcryptonews.ru/img/documets/What_Blockchain_Means_for_the_Sharing_Economy.pdf).

[380] Marten Risius & Kai Spohrer, A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There, Business & Information Systems Engineering, December 2017, Vol. 59, Issue 6, pp. 385-409.

[381] "Disruption" can be defined as a predictable pattern; to make it possible for something new and small to penetrate something existing and big in a short period of time. Jan Veuger, Trust in a viable real estate economy with disruption and blockchain, Facilities, 2018, Vol. 36, Issue 1/2, pp. 103-120, at p. 105 (https://doi.org/10.1108/F-11-2017-0106); The Economist, If blockchains ran the world: Disrupting the trust business, July 15, 2017 (available at https://www.economist.com/the-world-if/2017/07/15/disrupting-the-trust-business).

[382] As Botsman has aptly put it, the sharing economy lacks a shared definition. Rachel Botsman, The Sharing Economy Lacks A Shared Definition, Nov. 21, 2013, available at https://www.fastcompany.com/3022028/the-sharing-economy-lacks-a-shared-definition. "Sharing" has been defined as an alternative form of distribution to commodity exchange and gift giving or the act and process of distributing what is ours to others for their use and the act and process of receiving something from others for our use. Russell Belk, Why Not Share Rather Than Own? The ANNALS of the American Academy of Political and Social Science, Vol. 611, Issue 1, May 1, 2007, pp. 126-140, at pp. 126, 127. And economy can be understood as a system of trade and industry by which the wealth of a country is made and used. See Cambridge dictionary (https://dictionary.cambridge.org/dictionary/english/economy).

[383] Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, Simon Malone, Blockchain – The Gateway to Trust-free Cryptographic Transactions, Twenty-Fourth European Conference on Information Systems (ECIS), Istanbul, Turkey, 2016, pp. 1-14, at p. 2, available at https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2016_rp.

[384] Sinclair Davidson, Primavera De Filippi, Jason Potts, Economics of Blockchain, March 8, 2016, available at https://ssrn.com/abstract=2744751 or http://dx.doi.org/10.2139/ssrn.2744751, pp. 1-23, at p. 5.

[385] Benedikt Notheisen, Jacob Benjamin Cholewa, Arun Prasad Shanmugam, Trading Real-World Assets on Blockchain, An Application of Trust-Free Transaction Systems in the Market for Lemons, Business & Information Systems Engineering, December 2017, Vol. 59, Issue 6, pp. 425-440.

threaten privacy); smart contracts cannot trigger themselves, as they require explicit interventions[386]; blockchain relies solely on the correctness of predefined rules (that need to be secure, reliable and accurate)[387]; technical problems[388] might occur with regard to scalability, latency or query issues; and consensus algorithms might involve additional costs[389].

Besides, to some commentators, most of the features that are stated as intrinsic, like "immutable"[390] or "exact copy", are not intrinsic, but desired or emergent properties of a system, which involves many users, some of which might not be trusted[391]. A blockchain may, indeed, be ordered, digital, or cryptographically verifiable, albeit, other features (e.g. "distributed" or "mutable by-proof-of-work") are not features of a blockchain, but characteristics added by sharing, distribution, communication, and protocols[392]. Authors have also questioned the "speed of convergence" and the "size of the consensus", which are not by construction properties[393]. The reduction of energy might also be questionable, as the use of more computing nodes might result in the opposite[394].

---

[386] Florian Glaser, Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis, in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, pp. 1543-1552, at p. 1547 ("[…] *There is no self-execution at a certain point in time or environmental event without explicit external intervention* […]"). Available at https://pdfs.semanticscholar.org/859d/0535e16095f274df4d69df54954b21258a13.pdf.

[387] Sapumal Ahangama and Danny Chiang Choon Poo, Credibility of Algorithm Based Decentralized Computer Networks Governing Personal Finances: The Case of Cryptocurrency, in International Conference on HCI in Business, Government, and Organizations, HCIBGO 2016: HCI in Business, Government, and Organizations: eCommerce and Innovation (available at https://link.springer.com/chapter/10.1007/978-3-319-39396-4_15), pp. 165-176, at pp. 166-167, 173.

[388] Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, Simon Malone, Blockchain – The Gateway to Trust-free Cryptographic Transactions, id, at p. 11.

[389] Karl J. O' Dwyert and David Malone, Bitcoin Mining and its Energy Footprint, in 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies, ISSC 2014/CIICT 2014 (available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6912770).

[390] Immutability and security may be exaggerated. As blockchain is powered by the consensus protocol (proof-of-work), its "history" could be rewritten by attackers, who would control more than the half of the proof-of-work resources. See, amongst others, Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli, A Survey of Attacks on Ethereum Smart Contracts (SoK), in Maffei M., Ryan M. (eds), Principles of Security and Trust, POST 2017, Lecture Notes in Computer Science, Vol. 10204, Springer, Berlin, Heidelberg, pp. 164-186.

[391] As some have put it, trust is not created by a technology. Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, id, at p. 360 (mentioning that blockchain technology can facilitate better control and audit which ultimately might lead to some level of trust).

[392] Daniel Conte de Leon, Antonius Q. Stalick, Ananth A. Jillepalli, Michael A. Haney, Frederick T. Sheldon, Blockchain: properties and misconceptions, Asia Pacific Journal of Innovation and Entrepreneurship, 2017, Vol. 11, Issue 3, pp. 286-300, at pp. 288-290 (arguing that the "immutability" is an emergent property and that the statement that transactions "cannot be modified" is incorrect and misleading). See also at pp. 291-292, defining the emergent ledger or blockchain, in a Distributed Ledger System (DLS), as the resulting ledger, for which the majority (as defined by the DLS protocols) of the users agree at any given time.

[393] Daniel Conte de Leon, Antonius Q. Stalick, Ananth A. Jillepalli, Michael A. Haney, Frederick T. Sheldon, Blockchain: properties and misconceptions, id, at p. 292.

[394] Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, id, at p. 360 (arguing that blockchain technology is still evolving and thus subject to change).

And one could further argue that, since there is no central authority, integrity of the system is also emergent, or that the blockchain cannot be unique, since not all users may, in all cases, observe the same blockchain at the same time[395]. Furthermore, a blockchain's trustworthiness could be doubted, as smart contracts, implemented by code, may contain malicious flaws[396] and, hence, malicious actors might control others' actions.

So, it seems that the goals of a blockchain should not be regarded as its actual, existing, and intrinsic properties. There are some uncertainties and further experimenting would be needed to fully understand its possibilities and its limitations[397]. To some, blockchains are here to stay; to others, they are just a bubble[398]. Blockchains could be here to stay, as they could be effectively applied in multiple fields, such as music distribution or, in general, intellectual property management. But they would most probably fail to address the aspects of the personal data protection problem. One could fairly argue that, since smart contracts establish a digital relationship between two parties[399], the aspect of otherness would most probably not be addressed; third parties would be excluded. The fact that a blockchain is decentralized would, perhaps, mean that there would be no single identifiable entity responsible for the data processing. And this may further threaten people's control over their information. Besides, transparency that a blockchain promotes[400] might render data accessible by absolutely everyone; no room for secrecy and no space for those who would argue for the right to be forgotten. Equality, in its broader sense, might also be threatened, as not everybody has Internet access, albeit, blockchain is an

---

[395] Daniel Conte de Leon, Antonius Q. Stalick, Ananth A. Jillepalli, Michael A. Haney, Frederick T. Sheldon, Blockchain: properties and misconceptions, id, at p. 294.

[396] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, Elaine Shi, Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, 2015, pp. 1-15, at pp. 7-8. Available at https://eprint.iacr.org/2015/460.pdf. See also Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, id, at p. 181, whose system includes mobile phone users and entities, entrusted with maintaining the blockchain.

[397] To some, blockchains could provide some kinds of accountability: once an agent performs an action, others could be certain that she performed this action. Maurice Herlihy, Mark Moir, Blockchains and the Logic of Accountability: Keynote Address, id, at p. 27 (focusing on challenges concerning authorization, fairness, and incentives). To Herlihy and Moir, accountability could be proactive (in the sense that e.g. a Bitcoin balance would be transferred only if an agent established that it had been authorized) or reactive, meaning that a tamper-proof audit trail would allow after-the-fact analysis of actions, determining who did what and punishing the guilty. Perhaps, in this latter scenario, a mechanism for penalizing would be needed. But pro-active accountability mechanisms could also be developed in both permissioned or permissionless blockchains to block bad behavior (e.g. via ignoring double spending transaction as regards Bitcoin) or reward good behavior (for instance, via transactions that would pay successful Bitcoin miners).

[398] For an apt definition of irrational and rational bubbles (the "*bread and butter of monetary theorists*"), see Stephen Williamson, Is Bitcoin a Waste of Resources?, id, at p. 111 (with further references), mentioning modern fiat money as an example of (rational) bubble, which has no explicit future payoffs, yet we value it in exchange. To the author, a rational bubble occurs when an asset's value exceeds the present value of the expected future payoffs on the asset, appropriately discounted; irrational bubbles are supported by irrational behavior on the part of at least some market participants; "[…] *savvy investors ultimately end up selling all of the supply of the bubble asset to irrational people, who end up holding the bag when the price goes to zero* […]".

[399] Nick Szabo, Formalizing and securing relationships on public networks, First Monday, Vol. 2, No. 9 (Sep. 1, 1997), available at http://ojphi.org/ojs/index.php/fm/article/view/548/469; Ethereum, Introduction to smart contracts (2016-2018), available at http://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html.

[400] Scott J. Shackelford & Steve Myers, Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace, id, at p. 356.

online ledger. So, the equal distribution of personal data's value might not be achieved. Further uncertainties might occur, since smart contracts, not being contracts in the traditional sense, but a mere code, would carry out the function of legal contracts. So, what would happen if a transaction went wrong[401]?

Maybe, we need entities, neutral authorities, or data fiduciaries, in which the parties to the transaction would have some degree of trust and confidence. One may not trust the person that she is trading with, but she would trust that, if the trustee did not fulfil the obligation, someone would step in and enforce trade[402].

To those who argue for blockchains, the latter could return humanity back to the trust and transparency of transactions based on reputation, not mediated by third parties, whose interests may not be congruent with our own[403]. But we are always buying products or services, not the story behind them; with blockchain, one would be able to see the whole transaction and chain history of how the service or product came to be. If one drank a beer, she would be able to see the farmer who collected the cereal grains. But, likewise, the farmer might be able to see her.

What would this mean for personal data?

Maybe, we need more "dead bodies" in fields of privacy[404] to better understand the need for its reconceptualization[405]. Perhaps, everyone's concern needs to become, at least, someone's business[406]. And it might be true that privacy has been declared dead ever since it was conceived[407].

---

[401] Polly Botsford, Everywhere in chains, 71 No. 4 IBA Global Insight 16, available at https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=66b37621-c35e-4355-9420-16694b75263a.

[402] Mark D. Hansen & Michael Kokal, The Coming Blockchain Disruption: Trust without the "Middle-man", Business Litigation Committee Newsletter, December 2017, available at https://www.iadclaw.org/securedocument.aspx?file=1/19/Business_Litigation_December_2017.pdf.

[403] However, in this scenario, being fair and trustworthy might not suffice; perhaps, the system would also need to be able to prove to its customers its fairness and its trustworthiness. And its clients might include several types: "byzantine clients" (capable of arbitrary behavior, including malicious or malfunctioning nodes); altruistic clients (who could be trusted to follow the protocol); and rational clients (attempting to maximize a known objective function). Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Mike Dahlin, Jean-Philippe Martin, Carl Porth, BAR Fault Tolerance for Cooperative Services, SOSP '05 Proceedings of the twentieth ACM symposium on Operating systems principles, Brighton, United Kingdom, October 23-26, 2005, available at http://www.cs.cornell.edu/lorenzo/papers/sosp05.pdf, pp. 45-58, with further references.

[404] "[…] *its lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other categories of tort law* […]" Ann Bartow, A Feeling of Unease About Privacy Law, University of Pennsylvania Law Review / PENNumbra, 2006, Vol. 155, pp. 52-62, at p. 62.

[405] As some have argued, in contemporary information societies, maybe, we should treat the right to privacy and the protection of personal data as a fundamental right to the appropriate flow of information; perhaps, it is about contextualization of data that will in turn ensure this appropriate flow. Namely, it would be fair to argue that, in a job interview context, flow of data concerning an individual's marital status would probably be inappropriate. But the flow of same data in a different context, such as the context of courtship, would very likely be appropriate. Helen Nissenbaum, Privacy in Context, Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009, at pp. 127-230. As Nissenbaum argues, one could determine whether the information flow, in a given context or from one to another, is appropriate by applying the contextual integrity framework. This means identifying whether a specific information flow infringes an entrenched "context-relative" informational norm. Such norms (meaning prescriptive standards) are these, which are specifically concerned with the information flow in a given context. Thus, identification of norms requires

But there is one more reason to believe that personal data fiduciaries and fair play would most probably address the problem. It is the very theory, underpinning the fair information principles (the cornerstone for guidance[408]), that structures norms and statutes all over the world[409]. These principles give rights to data subjects and impose duties on data processors. And there is a remarkable consensus on basic legal principles[410], which could even lead to harmonization of international data protection laws, the tool for maintaining the health of the world's Internet-based economy[411]. Transparency, on which all privacy protection laws are based, establishes a relationship of trust; and this, reinforcing powerful social norms, is at the heart of the theory of information privacy[412].

Although only mathematicians can prove things using pen and paper and the rest of us have to take ideas pragmatically into the real world and see what works[413], albeit, to gain respect a model must explore unknown territories and foretell observations not yet made. By exposure to potential falsification a theory can prove its worthiness and can be then accepted as a useful working model of the world[414].

So, let us step into worlds of magic and territories of trust and fairness, before we are used to the idea that we no longer have any meaningful secrets.

---

identification of the context. Within the latter, informational norms depend on identification of subjects, senders and recipients, and relevant transmission principles, e.g. legal constraints. While determining the above norms it is important to detect the attributes, type, and nature of the information. Depending on the context, a specific item of information may or may not be considered appropriate according to the relevant context-relative informational norms.

[406] As Floridi has put it, everyone's concern is usually nobody's business. Luciano Floridi, Information ethics: On the philosophical foundation of computer ethics, id, at p. 37.

[407] Bart van der Sloot, The Individual in the Big Data Era: Moving towards an agent-based privacy paradigm, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 177-203, at p. 177 (mentioning that already in the sixties of last century authors proclaimed the end of privacy).

[408] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, id.

[409] Colin J. Bennett & Robin M. Bayley, Privacy protection in the era of 'Big Data': Regulatory challenges and social assessments, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds), Exploring the boundaries of Big Data, id, pp. 205-227, at pp. 208-209 (arguing that the simplicity of these principles would enable anyone to apply a "none of your business" test).

[410] See Colin J. Bennet, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, 1992, Cornell University Press, at p. 96 ("[…] *while the nomenclature and codification may vary from country to country, the substance and purpose of these principles are basically the same* […]").

[411] Steven C. Bennett, The "Right to Be Forgotten": Reconciling EU and US Perspectives, Berkeley Journal of International Law, 2012, Vol. 30, No. 1, pp. 161-195, at p. 174 (with further references).

[412] Colin J. Bennett & Robin M. Bayley, Privacy protection in the era of 'Big Data': Regulatory challenges and social assessments, id, at p. 209.

[413] David Brin, The Transparent Society, id, at p. 18.

[414] Some philosophers regard "prediction" as one true test of any theory. See, in general, Karl Popper, The Logic of Scientific Discovery (Logik der Forschung, first published 1935 by Verlag von Julius Springer, Vienna, Austria; later edition published by the Taylor & Francis e-Library, 2005, available at http://strangebeautiful.com/other-texts/popper-logic-scientific-discovery.pdf).

Editorial Board

ISBN 978-0-9784301-2-2 (Print)
ISBN 978-0-9784301-3-9 (Ebook)

Published by OABooks (The Canadian Center of Science and Education)

1120 Finch Avenue West

Suite 701-309

Toronto, ON., M3J 3H7

Canada